SÉCURISATION WINDOWS

Protégez efficacement votre infrastructure Windows

Code : SW

Ce cours vous confrontera à la mise en place de la sécurité des systèmes Windows. Il vous permettra de définir une politique de sécurité efficace en fonction des composantes du réseau d'entreprise. Les principales vulnérabilités du système et les problèmes de configuration seront étudiés et les corrections et bonnes pratiques à appliquer seront vues. Des protections mises en place par le système d'exploitation seront étudiées et analysées. La mise en place d'un domaine peut amener à des erreurs de configuration et des bonnes pratiques doivent être appliquées afin d'optimiser la protection des postes. L'utilisation des GPO permet de les appliquer de manière automatique sur l'ensemble du parc et de forcer les clients à appliquer des principes de sécurité.

PROGRAMME

Méthodes mobilisées : Cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (70% d'exercices pratiques) et formalisés sous forme de grille d'évaluation des compétences en fin de module par le formateur.

JOUR 1

Introduction

Enjeux et principes de la sécurité des systèmes d'information
- Défense en profondeur
- Politique de sécurité
  - Politique de mise à jour
  - Politique de sauvegarde
  - Politique de mots de passe
  - Politique de filtrage réseau
  - Politique de gestion des droits
  - Politique de journalisation
  - Politique de gestion des incidents
- Sensibilisation et formation

Durcissement du démarrage
- BIOS
- UEFI
- DMA
- Mesures de protection
  - BIOS / UEFI
  - DMA
  - Chiffrement du disque

Durcissement d'un environnement Windows
- Authentification Windows
- Mise à jour d'un système Windows
- Supervision
- PowerShell
- Protection des postes clients
  - Résolution de nom
  - Pile IPv6
  - SmartScreen
  - AppLocker
  - UAC
  - Device Guard
  - Credential Guard

JOUR 2

Durcissement d'un environnement Windows
- Active Directory
  - Introduction
  - Kerberos
  - Outils d'audit
  - Stratégies de groupe
  - **LAPS**

JOUR 3

Durcissement de services
- Principe du moindre privilège
- Autorité de certification
- Domain Name System (DNS)
- Service Message Block (SMB)
- Remote Desktop Protocol (RDP)
- Microsoft SQL (MSSQL)
- Lightweight Directory Access Protocol (LDAP)

PROCHAINES DATES

8 juin 2022,
3 oct. 2022

OBJECTIFS

- Savoir durcir et exploiter le démarrage d'un système
- Savoir durcir et exploiter un environnement Windows
- Connaître les méthodes d'attaques d'un Active Directory et comment s'en protéger
- Savoir durcir et exploiter les services Windows

INFORMATIONS GÉNÉRALES

Code : SW
Durée : 3 jours
Prix : 1 950 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois-Perret (92)

PUBLIC VISÉ

- Auditeurs techniques
- Administrateurs système

PRÉ-REQUIS

- Notions de sécurité informatique
- Connaissance des protocoles réseaux TCP/IP
- Maîtrise des systèmes Windows (client et serveur) et Active Directory
- Savoir développer des scripts.

RESSOURCES

- Support de cours
- 70% d'exercices pratiques
- 1 PC par personne / Internet
- Environnement Windows de démonstration (Windows 7, 10, server 2016) et Kali Linux