Formation « Sécurisation des infrastructures Windows »

Réf : SECUWIN

Système d'exploitation le plus utilisé dans l'entreprise et au dehors, et sans aucun doute l'un des plus attaqués, Windows est un composant incontournable de la majorité des systèmes d'information. Ancien "mauvais élève" de la sécurité, Microsoft a depuis quelques années mis la sécurité au centre de sa stratégie, avec pour résultat une grande diversité de mesures, parfois mal connues ou sous-utilisées, et de vraies avancées technologiques.

En vous apportant la maitrise de ces mécanismes de sécurité et la connaissance des techniques d'attaques usuelles, cette formation vous donnera les moyens de sécuriser et d'auditer votre infrastructure Windows avec un maximum d'efficacité.

Objectifs

- **Durcir un serveur Windows**
- **Administrer de façon sécurisée**
- **Sécuriser vos postes de travail**
- **Auditer votre infrastructure**

Durée & horaires

- **5 jours soit 40 heures**
- **Du lundi au jeudi : de 9h00 à 12h et de 13h30 à 19h00.**
- **Le vendredi : de 09h00 à 12h et de 13h30 à 17h00/17h30.**

Nombre de participant

- **Minimum 6 participants – Maximum 24 participants**

Public visé

- **Administrateurs**
- **Architectes**
- **Experts en sécurité**
- **Responsables sécurité**

Pré-requis

- **Formation SECUCYBER**
- **(ou) Expérience d'administration d'infrastructure Windows**
- **(ou) Solides bases en sécurité des systèmes d'information**

Méthode pédagogique

- **Cours magistral illustré par des travaux pratiques réguliers**

Supports

- **Support de cours au format papier en français**
- **Ordinateur portable mis à disposition du stagiaire**
- **Cahier d'exercices et corrections des exercices**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUWIN par HS2.**

Programme

Introduction

Module 1 : Durcissement système et réseau

- Système
  - Nécessité du durcissement
  - Minimisation
  - Gestion des services
  - Journalisation
- Réseau
  - Utilité des protocoles obsolètes
  - Cloisonnement réseau
    - Parefeu et IPsec
  - Protocoles d'authentification
  - Autres points d'attention
- Desired State Configuration
- Focus : sécuriser votre cloud Microsoft

Module 2 : Administration sécurisée

- Qu'est-ce qu'un administrateur
- Administration sécurisée : pourquoi ?
  - TTP : Techniques, Tactiques et Procédures
  - Compromettre un Active Directory
    - Compromission initiale
    - Mouvement latéral : Pass-the-hash...
    - Élévation de privilèges
  - Vulnérabilités classiques
- Bonnes pratiques
  - Utilisateurs et groupes locaux
  - Délégation
    - Powershell et le JEA
    - Active Directory et les GPO
- Administration sécurisée
  - Forêt "bastion"
  - Administration en strates
    - Silos d'authentification
  - Environnement d'administration
- Focus : Golden Ticket et krbtgt

Module 3 : Sécurité du poste de travail

- Windows 10 et le VBS
  - Secure Boot
  - Device Guard
  - Application Guard
  - Exploit Guard
  - Credential Guard
- Bitlocker
  - Chiffrement de disque
  - Autres fonctionnalités
- Isolation réseau
- Mise à jour

Module 4 : Auditer son infrastructure

- Différents types d'audits
- Points à auditer
- SCM
- Pingcastle
- Recherche de chemins d'attaque
  - BloodHound et AD-Control-Path
  - Les extracteurs
  - Graphes d'attaques
  - Simulation et remédiation
- Examen