SÉCURITÉ WINDOWS & ACTIVE DIRECTORY

Comprendre et pratiquer les attaques spécifiques aux infrastructures Windows Active Directory

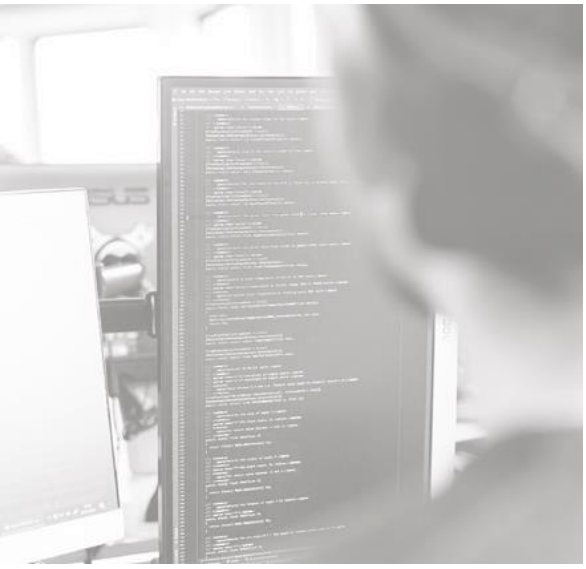
Ce cours vous confrontera aux enjeux de sécurité de la mise en place d'infrastructures Windows Active Directory.
Il vous permettra d'appréhender l'intérêt de politiques de sécurité efficaces en fonction des actifs du réseau d'entreprise.
Les principales vulnérabilités des systèmes et les problèmes de configuration seront vues et exploitées.
Corrections, bonnes pratiques et protections seront étudiées et analysées.
En effet, la mise en place d'un domaine peut amener à des erreurs de configuration.
Les sujets seront abordés de manière didactique et interactive, sous forme théorique et pratique, en fournissant un environnement de hacking dédié à chaque élève depuis notre plateforme de cyber-entraînement Malice.

Code : SWAD

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 complétée 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

Sécurité 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

Sécurité d'un environnement Windows (suite)

- Active Directory
  - Introduction
  - Kerberos
  - Outils d'audit
  - Stratégies de groupe
  - LAPS

JOUR 3

Sécurité des 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

5 juin 2024
13 novembre 2024

OBJECTIFS

- Savoir exploiter les faiblesses de configuration du démarrage d'un système
- Comprendre et exploiter les faiblesses des environnements Windows & Active Directory
- Connaître les méthodes d'attaques d'un Active Directory et comment s'en protéger
- Savoir durcir et exploiter les services Windows

INFORMATIONS GÉNÉRALES

Code : SWAD
Durée : 3 jours
Prix : 2 300 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) ou en distanciel

PUBLIC VISÉ

- Auditeurs techniques en devenir
- Administrateurs système

PRÉ-REQUIS

- Avoir des notions de sécurité informatique
- Avoir des connaissances en protocoles réseaux TCP/IP
- Avoir des connaissances sur les systèmes Windows (client et serveur) et Active Directory
- Avoir des notions de développement de scripts

Un niveau HSA est recommandé afin de suivre confortablement la formation.

RESSOURCES

- Support de cours
- 70% d'exercices pratiques
- 1 PC par personne
- Environnement Windows de démonstration et Kali Linux