

Sécurité dans Vista SP1 – EIG

Programme du 1^{er} jour

08h30 Introduction

09h00 **1) Sécurité utilisateur (théorie)**

- Whoami → Utilisateur, Groupe, SID, jeton (droits)
- UAC (*User Account Control*)
Pourquoi ? Moindre privilège
Comment ? *Manifest*
10 paramètres de *Local Policies – Security Options*
- *Application Compatibility Tool*
- Liens

10h15 **Labo1 : User Account Control**

- Privilèges de comptes & groupes (*User Right Assignment*)
- Moindre privilège
- Niveaux d'exécution des applications
- Forcer une application à s'exécuter avec des privilèges élevés
- Configurer UAC avec les *Security Policies*
- Désactiver UAC de manière temporaire / permanente

11h00 **2) Firewall (théorie)**

- Réseaux (interfaces physiques, profils, outils)
- *Firewall* (règles, outils GUI & CLI, logs)
- Autres fonctions

11h30 **Labo2 : Firewall**

- Gérer les profils réseau
- Configurer le *firewall* afin d'obtenir un accès *web*
- Contrôle des applications par le *firewall*
- Netsh

14h00 **3) System Architecture (théorie)**

- Principales différences par rapport à XP
- *Boot, Code Integrity, Device Installation Restrictions, Windows Resource Protection*
- Processus, comptes système, sessions, services, *service hardening*
- *Winlogon, Windows Station, Desktop, Window, Token*
- *Mandatory Integrity Control (No write-up)*
- *Shatter attack & User Interface Privilege Isolation*
- Liens

15h15 **Labo3 : System**

- *Boot* (processus, comptes système, session utilisateur, authentification, services)
- *Windows Service Hardening*
- *Mandatory Integrity Control* (isolation des processus, contrôle d'accès des objets)
- *Code Integrity* (signature des exécutables, autoriser / interdire l'installation d'un périphérique, audit)
- *Windows Resource Protection*

Programme du 2^{ème} jour

08h30

4a) Principes de sécurité (théorie)

- Principaux risques
- 7 principes de sécurité
- Liens

09h00

4b) *Security Guide & Hardening*

- *Windows Vista Security Guide* (contenu, Gpedit, mise à jour SCE, *security options*)
- ACL et service *TrustedInstaller*
- *Software Restriction Policy* (SRP)

09h30

Labo4 : *Vista Hardening*

- Restreindre les droits des utilisateurs
- Définir les options de sécurité
- Modifier les ACL
- Désactiver les services inutilisés
- Configurer SRP
- Imposer une politique de mot de passe
- Protection de l'identité des utilisateurs lors du *login*

11h00

5) Déploiement (théorie)

- Déploiement
- Qu'est ce qu'une image ?
- Format d'image *WIM* dans Vista
- *ImageX*
- *Windows PE 2.0*
- Fichiers de réponse (*Unattend.xml*)
- Phases de configuration
- *Windows System Image Manager*
- Serveur *WDS* (*Windows Deployment Services*)

11h30

Labo5 : Déploiement

- *Windows PE*
- Gérer les images *WIM*
- Images utilisées lors des labos
- Ajouter un *driver* à une image en mode *offline*
- Configurer et automatiser une installation Vista
- Utiliser un fichier de réponse lors de l'installation d'une image
- Préparer un système pour son déploiement

15h30

6) Divers

- Activation
- BitLocker
- *Network Access Protection* (NAP)
- CardSpace
- Versions de Vista
- Mon matériel supporte-t-il Vista ?
- IE7
- Liens & Remarques

16h15

Labo6 : *IE7*

- Renforcer la sécurité de *IE7*