TP2 - Script de collecte de configuration et d'une documentation technique associée

William Boisseleau

2024-10-10

XMCO - Université de Rouen

Consignes à respecter

Consignes à respecter

Sur le fond

Pour ce TP :

- l'accès à Internet est autorisé
- Le copier/coller ne l'est pas, si ce n'est pour les termes attendus
- Dans votre rapport final **citer systématiquement** vos sources (lien direct).
- **Toutes les commandes** utilisées **doivent être incluses** dans votre rapport
- Illustrez votre rapport par **des captures d'écran** et liste des commandes exécutées
- Expliquez votre démarche systématiquement au sein du rapport

Consignes à respecter

Sur la forme

- Déposez 1 seul fichier par équipe de 2 sur Universitice : **archive de données** : `M2SSI-SECURITE_WINDOWS-TP2-NOM1_PRENOM1-NOM2_PRENOM2.zip`. Celle-ci contient :
  - Rapport au**format pdf** : `M2SSI-SECURITE_WINDOWS-TP2-NOM1_PRENOM1-NOM2_PRENOM2.pdf`. Le rapport doit contenir captures d'écrans / commandes / notes rédigées / réponses aux questions.
  - Annexes techniques et documentaires (scripts)
- **Deadline forte** : Spécifiée sur le **formulaire de dépôt Universitice**

Je reste à votre disposition durant le cours, ou à l'issue si vous avez la moindre question (`william.boisseleau2@univ-rouen.fr`).

Sujet TP2

Contexte

Vous êtes **auditeur sécurité**. Un client vous demande de réaliser un **audit de configuration** sur un serveur Windows, **audit réalisé à froid** (sans accès direct au serveur).

Vous êtes missionnés en équipe de 2 pour cet audit.

Vous devez transmettre au client (moi-même) un **script** vous permettant de réaliser l'audit de configuration *[partie 1]* ainsi qu'une **documentation complète associée** (orientée intérêt sécuritaire de la collecte) *[partie 2]*.

Partie 1

- *Partie 1* et *Partie 2* à traiter par **groupe de 2**
  - Désignez un **chef de projet** en charge de la communication / échanges par mail (Correspondant au `Nom1 Prenom1`)
  - A la remise des livrables, le chef de projet **devra rappeler avec qui il était**
- En vous appuyant sur les thématiques sécurité vues en cours, réalisez **un outil de collecte de configuration Windows** en VBScript.
- Le script doit être **autoporteur**
  - il ne prend aucune entrée utilisateur et doit être lancé depuis un `cmd`. Il doit supporter tous les systèmes Windows, depuis Windows Server 2008.
  - il doit générer localement des traces (informations utiles d'un point de vue de la sécurité) pour une analyse de ces traces à froid (a posteriori)
  - Regroupez automatiquement les traces générées dans une archive native au système (non zip)
- La **qualité de code** sera considérée dans la notation (documentation / nommages explicites / segmentation par fonction / logique de collecte / etc.)

Partie 2

- Rédigez un **rapport justificatif du script** annexe au code VBScript :
  - Documentez rapidement l'architecture de votre script (diagrammes / explication de la logique succincte ; 1 page maximum)
  - Pour **chaque commande exécutée** (et présente dans votre script), expliquez
    - Ce que retourne la commande
    - Pourquoi vous récupérez cette information (intérêt sécuritaire et de contrôle). Les données collectées doivent être systématiquement justifiées dans la documentation

Sujet TP2

Partie 2

NB1 : Il ne s'agit que d'un script de collecte, pas un script d'analyse
NB2 : Soignez votre script et votre rapport ; ils pourront vous être utiles a posteriori