TP1 - Installation d’un serveur Windows

William Boisseleau

2024-09-20

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
- Pour toutes vos réponses, merci de **citer systématiquement** vos sources (lien direct).
- **Toutes les commandes** utilisées pour la réponse **doivent être incluses** dans votre rapport
- Illustrez votre rapport par **des captures d'écran** et liste des commandes exécutées
- Expliquez votre démarche systématiquement

Consignes à respecter

Sur la forme

- Déposez 1 seul fichier sur Universitice : **archive de données** : `M2SSI-SECURITE_WINDOWS-TP1-NOM_PRENOM.zip`. Celle-ci contient :
  - Rapport au**format pdf** : `M2SSI-SECURITE_WINDOWS-TP1-NOM_PRENOM.pdf`. Le rapport doit contenir captures d'écrans / commandes / notes rédigées / réponses aux questions.
  - Annexes techniques et documentaires (scripts)
- **Deadline** : **2024/09/27 - 9H00**

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

Questions TP1

Questions TP1

- **1.** Installez Virtualbox et ses extensions. Téléchargez Windows Server 2012 R2 (version d'essai - langue anglaise)
- **2.** Créez un environnement virtuel pour Windows sur Virtualbox. Documentez vos choix concernant les ressources attribuées à la machine virtuelle en vous appuyant sur des ressources officielles. Expliquez votre choix de configuration Réseau.
- **3.** Montez le disque téléchargé sur la VM et lancez la machine virtuelle. Installez le serveur Windows Server 2012 R2 avec Interface Graphique
- **4.** Créez un compte administrateur. Justifiez votre choix de nommage. A la fin de l'installation, effectuez une snapshot de la machine.
- **5.** Créez un répertoire d'échange (*shared folder*) entre votre machine hôte et votre machine virtuelle. Assurez-vous que vous êtes bien en mesure d'échanger des données entre votre hôte et la VM.
- **6.** Ouvrez l'intepréteur de commande par défaut de Windows. Identifiez les commandes adaptées qui permettent d'afficher les informations suivantes :
  - l'utilisateur courant
  - la liste des utilisateurs locaux
  - la liste des groupes locaux
  - la version du système
  - informations détaillées sur les interfaces réseau configurées
  - la liste des processus en cours d'exécution
  - la liste des services en cours d'exécution

Questions TP1

- **7.** Identifiez 3 services en cours d'exécution sur le serveur (au choix, services vous semblant intéressants). Décrire ces services, leurs usages. Identifiez les documentations officielles respectives, utiles pour un durcissement de ces services.
- **8.** Créez via l'instance 4 comptes supplémentaires sur le système :
  - 1 compte administrateur supplémentaire
  - 2 comptes standards au sein d'un groupe `M2SSI`
  - un compte standard dans le groupe `STAGIAIRE` au mot de passe `Password01!`
    Listez tous les comptes et groupes créés.
- **9.** Où sont stockés les comptes et leurs secrets configurés sur le système de fichier ? Proposez 2 méthodes différentes pour récupérer ces fichiers pour une analyse à froid. Décrivez la démarche de récupération. Identifiez les noms d'utilisateurs et leur mot de passe stocké au sein de ces données.
- **11.** Dans quels formats sont stockés les mots de passe ? Que pouvez-vous dire de leur résistance au cassage ? Lancez un cassage de vos mots de passe avec l'outil de votre choix. Présentez les résultats

Questions TP1

- **12.** Qu'est ce que Powershell ? Identifiez des commandes spécifiques Powershell permettant de :
  - Lister les comptes sur le système
  - Lister les processus en cours d'exécution
  - Lister les mises à jour installées sur votre serveur
- **13.** Proposez une stratégie technique pour vérifier par analyse à froid que le système est à jour dans ses correctifs de sécurité.
- **14.** Qu'est ce que l'UAC ? Comment est-il configuré par défaut ? Quelles sont vos recommandations ? Appliquez-les.
- **15.** Installez un serveur IIS suivant votre serveur Windows. Configurez le en suivant les meilleures pratiques de sécurité. Expliquez votre démarche et votre mise en œuvre.
- **16.** Déposez une page Helloworld ASPX à la racine de votre serveur. Exposez cette ressource sur une interface réseau. Montrez que vous pouvez accéder à la page depuis votre système Hôte.
- **17.** Citez deux méthodes pour se connecter à distance sur votre serveur Windows (méthodes "nativement" supportées). Décrivez rapidement les 2 services / protocoles et les ports par défaut sur lesquels ils sont exposés. Depuis un hôte Linux, connectez-vous à distance à votre serveur en utilisant des clients initiés en ligne de commande.

Questions TP1

- **18.** Activez le service SMB sur le serveur. Créez un répertoire partagé `SHARED`, au sein duquel se trouvent deux répertoires `SECURED` et `PUBLIC`. Les administrateurs doivent pouvoir accéder en lecture/écriture aux deux répertoires à distance. Le répertoire `PUBLIC` doit être accessible en lecture seule (à distance) à tous les comptes locaux. Démontrez cette configuration, en réalisant un accès distant SMB depuis votre hôte, avec un compte administrateur local et un compte standard.
- **19.** BONUS - Implémentez un script VBS (en respectant les Bonnes Pratiques de développement), exécutant de manière automatique toutes les actions listées ci-avant.