AP16 : SAMBA & SECURITE SWITCHES

Présentation générale :

Vous êtes stagiaire chez la société MenuiMétal dont le PDG est Jean Morin. Vous êtes attaché au service informatique dirigé par Monsieur Olivier Lepage, votre tutrice est Catherine Bercy, assistante de M Lepage.
Monsieur Lepage s'interroge sur les solutions qui permettent d'unifier la gestion des utilisateurs, des données et sécuriser son infrastructure pour faire face à d'éventuelles menaces.

Mission 0 : Prérequis et contraintes

- Répartir les tâches via Gantt
- Mettre à jour le schéma réseau
- Les switches Cisco et HP sont configurés.
- Une VM avec Wireshark installé
- Cloner 2 VM linux, changer leur hostname (srv-samba et cli-samba) et les mettre dans le vlan LAN
- Cloner 1 VM Windows (win-smb), changer son hostname et la mettre dans le vlan LAN
- Remonter les VMs sur GLPI
- Accéder à la console des VMs via SSH pour Linux et RDP pour Windows

Mission 1 : SAMBA

Monsieur Lepage cherche à récupérer des données d'environnement hétérogène où l'on trouve des systèmes d'exploitation différents comme Linux ou Windows. Une des solutions possibles c'est d'utiliser SAMBA

1. Expliquer en quelques lignes le fonctionnement de SAMBA et ses avantages dans des environnements hétérogènes
2. Quel est le rôle d'un DC ?
3. Pourquoi le DNS et le temps sont des éléments importants dans la mise en place d'un AD-DC ?
4. Quel est le rôle des tickets Kerberos ?
5. Quel est le rôle du fichier `/etc/samba/smb.conf` ?
6. Mise en place de SAMBA en tant que serveur de fichiers sous Linux :
    - Configurer un partage avec SAMBA
    - Accéder au partage SAMBA depuis une machine Windows
    - Gérer les droits sur ce partage : réaliser au moins deux tests
7. Mise en place de SAMBA comme Contrôleur de domaine
    - Configurer Samba comme contrôleur de domaine
        - Utiliser le fichier `/etc/hosts` comme outil de résolution DNS
        - Vérifier :
            - L'état du service

            - La présence des enregistrements DNS avec la commande `host -t`
            - Le ticket Kerberos administrateur
        - Créer un OU nommée People
        - Créer des utilisateurs au moins quatre
        - Créer deux groupes : IT et Commercial
        - Affecter deux utilisateurs dans chaque groupe
        - Intégrer une machine Windows au domaine
            - Installer les outils RSAT
            - Mettre en place des GPO
                - Mapper un lecteur réseau sur les répertoires partagés
                - Changer le fond d'écran de tous les utilisateurs
8. Intégrer une machine Linux dans le domaine SAMBA avec SSSD
    - Expliquer le rôle de SSSD
    - Les home directory des utilisateurs sont montés automatiquement
9. Superviser la VM sur Nagios avec les plugins de base et spécifique à Samba
10. Remonter les logs du serveur Samba sur le serveur Rsyslog

Mission 2 : Sécurisation d'un équipement réseau

Une des références en matière de sécurité pour Monsieur Lepage c'est l'ANSSI. Il vous demande d'améliorer la sécurité des switches de l'environnement de Ménuimétal. Ses collaborateurs ont effectué des recherches sur Internet et parmi celles-ci ils ont trouvé des préconisations de l'ANSII dont le lien est ci-dessous :
https://cyber.gouv.fr/publications/recommandations-pour-la-securisation-dun-commutateur-de-desserte

Monsieur Lepage vous demande d'améliorer la sécurité des switches de Ménuimétal

1. Faire un résumé des préconisations de l'ANSSI sur les thèmes suivants :
    a. Les vlans
    b. Sur les commutateurs Cisco, différence entre le vlan par défaut et le vlan natif
    c. L'accès à distance aux switches avec des comptes locaux ou centralisés
    d. La sécurité des ports des switches
    e. L'intérêt de la journalisation
    f. A quoi sert le DHCP snooping
    g. En utilisant le protocole snmpv2c, quelle est la différence entre le mode get et trap ?
2. Vérifier que l'accès aux switches HP et Cisco peut se faire via Telnet et SSH
3. Ajouter un PC portable dans le vlan LAN, il obtiendra un IP dynamique via votre serveur DHCP sous Linux
4. Vérifier via Wireshark les trames concernant le serveur DHCP
5. Quelle est la commande à utiliser qui permet d'obtenir les adresses MAC acquises par les commutateurs ? Récupérer les adresses MAC acquises par vos switches
6. Faire un tableau récapitulatif du port, de l'adresse MAC et de l'hôte associé
7. Mise en place de la sécurité par port

a. Sécuriser manuellement le port associé au PC portable. Faire un test de fonctionnement
b. Sécuriser de façon dynamique le port associé au PC portable. Faire un test de fonctionnement
c. Mettre en place une solution de violation de sécurité

8. Sauvegarder les nouvelles configurations sur le serveur TFTP ou le serveur RANCID
9. Sur les journaux du commutateur remontés sur votre serveur de LOG :
    - Identifier les évènements liés au serveur DHCP
    - Repérer la sécurisation des ports de votre commutateur

REALISATION DU PROJET

1. Le travail s'effectuera en mode projet par équipe de 2 personnes. Chaque équipe devra s'organiser pour planifier le déroulement du projet et répartir les tâches.
2. La recette doit être finalisée pour le ***vendredi 20 mars 2026***
3. Vous devrez produire les éléments suivants :
    - Planning prévisionnel et réalisé du projet (liste des tâches et durées, répartition, GANTT)
    - Compte rendu du projet où l'on doit retrouver le déroulé de vos missions ainsi que les informations suivantes :
        - Liste et description des configurations effectuées (cf : Tuto)
        - Liste et description des erreurs et problèmes rencontrés et des solutions apportées
        - Documentation sur les tests que vous avez mis en place pour vérifier le bon fonctionnement des services