Rappel

Pour se connecter à la machine host :

```
 Enter-PSSession -HostName "DJ4JN202-AUT-1.numerilab-cesi.fr" -UserName "administrateur"
Enter-PSSession -MachineName SRV-AD.tp.local" -UserName "Administrateur"
```

TP 11 : Audit des comptes utilisateurs inactifs

- **Objectif :** Identifier les comptes qui n’ont pas été utilisés pour renforcer la sécurité.
- **Énoncé :** Listez tous les utilisateurs du domaine qui ne se sont pas connectés depuis plus de 90 jours. Affichez leur nom (`Name`), leur `SamAccountName` et la date de leur dernière connexion.
- **Indices :** `Get-ADUser` , paramètre `-Filter` , propriété `LastLogonDate` .

TP 12 : Cartographie des groupes d’administration

- **Objectif :** Vérifier qui possède des privilèges élevés sur le domaine.
- **Énoncé :** Affichez la liste des membres du groupe “Domain Admins”. Le script doit retourner uniquement le nom d’affichage (`DisplayName`) et l’état du compte (activé ou désactivé).
- **Indices :** `Get-ADGroupMember` , `-Identity "Domain Admins"` , `Get-ADUser` pour récupérer les détails de chaque membre.

TP 13 : Recherche de comptes “sensibles”

- **Objectif :** Isoler les comptes dont le mot de passe n’expire jamais dans l’AD.
- **Énoncé :** Identifiez tous les utilisateurs de l’AD ayant l’option “Le mot de passe n’expire jamais” activée. Exportez le résultat dans un fichier CSV nommé `Audit_Passwords.csv` .
- **Indices :** `Get-ADUser -Filter 'PasswordNeverExpires -eq $true'` , `Export-Csv` .

TP 14 : Analyse de l’arborescence des Unités d’Organisation (OU)

- **Objectif :** Visualiser la structure de l’annuaire.
- **Énoncé :** Listez toutes les Unités d’Organisation présentes dans le domaine. Pour chaque OU, affichez son nom et le chemin complet (`DistinguishedName`).
- **Indices :** `Get-ADOrganizationalUnit -Filter *` , `Select-Object Name, DistinguishedName` .

TP 15 : Audit du verrouillage des comptes

- **Objectif :** Identifier les utilisateurs actuellement bloqués suite à des erreurs de mot de passe.
- **Énoncé :** Écrivez un script qui recherche tous les utilisateurs dont le compte est actuellement verrouillé (`LockedOut`). Affichez l’heure du verrouillage.
- **Indices :** `Search-ADAccount -LockedOut` , `Select-Object Name, LockedOutPropertyValue` .

TP 16 : Rapport sur les ordinateurs du domaine

- **Objectif :** Inventorier le parc informatique enregistré dans l’AD.

- **Énoncé :** Listez tous les ordinateurs du domaine. Affichez leur nom, leur système d'exploitation et la version de l'OS. Triez le résultat par système d'exploitation.
- **Indices :** `Get-ADComputer -Filter * -Properties OperatingSystem`, `Sort-Object OperatingSystem`.

TP 17 : Vérification de l'appartenance aux groupes d'un utilisateur

- **Objectif :** Auditer les droits d'un utilisateur spécifique.
- **Énoncé :** Demandez (via une variable) le nom d'un utilisateur et listez tous les groupes de sécurité dont il est membre (groupes directs uniquement).
- **Indices :** `Get-ADPrincipalGroupMembership`, `Select-Object Name`.

TP 18 : Identification des comptes sans protection contre la suppression

- **Objectif :** Prévenir les erreurs de manipulation administratives.
- **Énoncé :** Trouvez tous les objets de type "Utilisateur" qui ne bénéficient pas de la protection contre la suppression accidentelle.
- **Indices :** `Get-ADUser -Filter * -Properties ProtectedFromAccidentalDeletion`, filtre sur la valeur `$false`.

TP 19 : Statistiques de création de comptes

- **Objectif :** Suivre l'évolution récente de l'annuaire.
- **Énoncé :** Affichez tous les comptes utilisateurs créés au cours des 30 derniers jours. Affichez la date de création et la personne qui a créé le compte (si l'attribut est renseigné).
- **Indices :** `Get-ADUser`, propriété `whenCreated`, calcul de date avec `(Get-Date).AddDays(-30)`.

TP 20 : Vérification de l'état des contrôleurs de domaine

- **Objectif :** S'assurer de la santé de l'infrastructure AD.
- **Énoncé :** Récupérez la liste de tous les contrôleurs de domaine de la forêt actuelle et affichez leur adresse IP ainsi que leur mode de fonctionnement (Global Catalog ou non).
- **Indices :** `Get-ADDomainController -Filter *`, `Select-Object Name, IPv4Address, IsGlobalCatalog`.