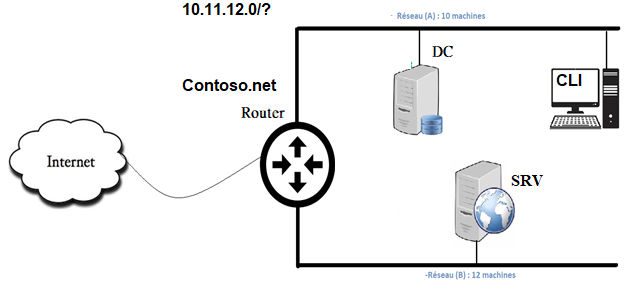
**Laboratoire #1**

****

1. **Besoin du laboratoire**Pour accomplir ce laboratoire vous aurez besoin des composants matériels et logiciels suivants :

* **Un serveur SRV :**  
  o OS : Windows Server 2016/2019 Datacenter  
  o Nom NetBIOS : SRVo NIC : 1 interface, @IP à déterminer selon le plan d’adressage du réseau (B);  
  o Machine ayant intégré au domaine : **Contoso.net**o Fonction : machine contenant un partage **SMB** et centralisant les journaux d’évènement des autres machines.
* **Un serveur Router :**o OS : Windows Server 2016/2019 Datacenter.  
  o Nom NetBIOS : **Router** *(non nécessairement intégré au domaine)*  
  o NIC : 3 interfaces, @IP à déterminer selon le plan d’adressage des 3 réseaux : (A), (B) et (E);  
  o Fonction : routage entre les réseaux et partage de connexion Internet.
* **Un serveur DC :**o OS : Windows Server 2016/2019 Datacenter  
  o Nom NetBIOS : **DC** *(Contrôleur de domaine :* ***Contoso.net****)*o NIC : 1 interface, @IP à déterminer selon le plan d’adressage du réseau (A);  
  o Machine jouant le rôle de contrôleur de domaine Active Directory.
* **Un client CLI :**o OS : Windows 10 Professionnel.  
  o Nom NetBIOS : **CLI** (machine jointe au domaine *:* ***Contoso.net***)o NIC : 1 interface, @IP à déterminer selon le plan d’adressage du réseau (A);

1. **Travail demandé :**

## **Première partie : Adressage et implantation et configuration des rôles** *(20 pts).*

* 1. Procédez au calcul du *Subnetting* pour distribuer l’adresse 10.11.12.0/? pour vos deux réseaux (A) et (B). (*Le signe ‘****?****’ indique que vous devriez choisir un masque de sous-réseau optimal pour chacun des sous réseaux*) ***(10 pts).***

L’attribution des adresses aux différentes interfaces des machines doit commencer par celles du routeur pour les deux réseaux (A) et (B).

Pour cela, vous devez remplir le tableau d’adressage des sous réseaux suivant :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Écrire Réseau   1. Ou (B) ? | NetID | 1ère Adresse utilisable | Dernière adresse utilisable | Masque de sous réseau (notation décimale) | Préfixe  (Notation CIDR) |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

***NB.****: Tenir en considération que le réseau (A) peut contenir jusqu’à 10 adresses IP y compris celle de l’interface du routeur* ***Router****. Aussi, le réseau (B) peut contenir jusqu’à 12 adresses IP y compris celle de l’interface du routeur* ***Router****.*

* 1. Toutes les machines doivent être opérationnelles selon les spécifications du besoin du laboratoire : ***(10 pts).***
     1. Pour la machine **CLI** faites les captures nécessaires qui montrent qu’elle est intégrée au domaine, qu’elle peut communiquer avec la machine SRV (ping) et qu’elle peut sortir sur Internet.
     2. Pour le contrôleur de domaine DC, faites les captures nécessaires qui montrent que le conteneur ***Computer*** contient les machines intégrées au domaine.
     3. Pour le serveur **Router,** faitesles captures nécessaires qui montre l’installation et la configuration du rôle du routage ainsi que le partage de connexion Internet.
     4. Pour le serveur **SRV,** faites une capture qui montre qu’elle peut sortir sur Internet.

## **Deuxième partie : Analyse du trafic lié au partage SMB *(40 pts)***

Pour satisfaire aux obligations de conformité, le trafic concernant le partage sur les réseaux (A) et (B) doit être chiffré de façon à le protéger des interceptions. Vous allez donc utiliser **Microsoft Message Analyzer** pour analyser le trafic réseau :

1. Utilisez le compte Administrateur de domaine pour installer **Microsoft Message Analyzer** sur la machine **SRV**.
2. Sur **SRV**, créez un dossier partagé nommé : **D :\Labo1**
3. Sur **SRV** et en tant qu’administrateur de domaine, procédez à la Capture du trafic réseau non chiffré en utilisant **Microsoft Message Analyzer** comme suit :
4. Sur **CLI** et en tant qu’administrateur de domaine, créer un fichier sur le Bureau, nommé **MonSecret.txt** et copier-le sur le partage **: \\SRV\Labo1**
5. Copiez aussi **C :\Windows\System32\WindowsCodecsRaw.txt** vers le dossier **\\SRV\Labo1**
6. Sur **SRV**, stopper la session dans **Microsoft Message Analyzer**
7. Appliquez un filtre qui montre seulement le trafic impliquant **CLI (***Triez sur l’en-tête* ***DiagnosisTypes****, puis examinez le trafic*.**)**
8. Appliquez le point de vue **SMB/SMB2**, puis examinez le trafic **SMB2.**
9. Créez une règle de couleur en utilisant la bibliothèque pour appliquer une certaine couleur au trafic contenant la chaîne **TXT**. Examinez les paquets auxquels cette couleur est appliquée.
10. Sur le contrôleur de domaine **DC**, Activer **IPsec** dans un objet de stratégie de groupe. *(N’oubliez pas de passer sur* ***CLI*** *et sur* ***SRV*** *pour forcer les mises à jour avec* ***GPUPDATE****.)*
11. Capturer de trafic du réseau chiffré : Sur **SRV**, dans **Microsoft Message Analyzer**, démarrez une nouvelle session qui utilise le scénario **Local Network Interfaces (Win 8.1 and later).**
12. Sur **CLI,** allez sur le partage **\\SRV\Labo1** et ensuite copiez le fichier **WindowsCodecsRaw.txt** sur le Bureau local.
13. Passez sur **SRV** pour stopper la session de **Microsoft Message Analyzer.**
14. Appliquez un filtre qui montre seulement le trafic impliquant **CLI.** *(Vous devez triez sur l’en-tête* ***DiagnosisTypes****, puis examinez le trafic.)*

***Remarque****: Vous devez remarquer que la plus grande partie du trafic capturé provient du module* ***ESP*** *(un protocole d’IPSec)*

1. Sur le contrôleur de domaine **DC**, désactiver **IPsec** dans un objet de stratégie de groupe. *(N’oubliez pas de passer sur* ***CLI*** *et sur* ***SRV*** *pour forcer les mises à jour avec* ***GPUPDATE****.)*

Maintenant, vous allez tester le chiffrement **SMB 3.1.1**. Vous utilisez Windows PowerShell pour activer un partage chiffré avec **SMB** sur un système Windows Server 2016/2019.

1. Pour vérifier que **IPsec** est bien désactivé, vous ne devez trouver aucun trafic capturé concernant le module **ESP**. Pour cela, vous devez lancer sur **SRV** une session de **Microsoft Message Analyzer.** Ensuite passer sur **CLI** pour copier vers le dossier **\\SRV\Labo1** les deux fichiers **MonSecret.txt** et **C :\Windows\System32\WindowsCodecsRaw.txt**
2. Sur **SRV**, et à l’aide de **Windows PowerShell**, créer le partage chiffré avec SMB, Nom du partage : **Labo1**, chemin du partage : **D :\Labo1**
3. En utilisant PowerShell, définissez toutes les permissions à **Tout le monde** pour le partage : **Labo1**.
4. Pour vérifier le chiffrement SMB, vous devez lancer sur **SRV** une session de **Microsoft Message Analyzer.** Ensuite passer sur **CLI** pour copier le fichier et **WindowsCodecsRaw.txt** depuis **\\SRV\Labo1** vers le Bureau local.
5. Appliquez un filtre impliquant la machine **CLI** et le protocole **SMB2**. Ensuite, cliquez sur l’en-tête **Summary** pour trier par module. Vous devez avoir la plus grande partie du trafic **SMB2** capturé : **TransformMessage, Encrypted**

## **Troisième partie : Transfert des journaux d’événements *(30 pts)***

1. Configurez les machines **DC** et **CLI** somme ordinateurs sources d’événements;
2. Activez **WinRM** en utilisant un GPO à appliquer sur une unité d’organisation contenant les ordinateurs : **DC** et **CLI**.
3. Définir le(s) membre(s) du groupe local Administrateurs des ordinateurs (**DC** et **CLI**) sources d’événements, pour cela utilisez un **GPO**.
4. Configurer **SRV** comme ordinateur collecteur d’évènements;
5. Créer et configurer un abonnement d’événement nommé : **LogLabo1**
6. Activer l’audit de création des utilisateurs sur **DC** et créer un utilisateur : **Bob;**
7. Sur **CLI**, Activer l’audit de l’accès à un répertoire (**c:\rep1**) et accédez à **c:\rep1** et y créer un fichier texte (**fich.txt**) et/ou un répertoire (**rep2**)
8. Tester la présence des événements de création de l’utilisateur Bob et celui d’accès et de création du fichier **fich.txt** sur le journal du collecteur **SRV**.

**Consigne du laboratoire :**

* Ce laboratoire peut être réalisé individuellement ou par équipe de 2 étudiants;
* La présentation du livrable est évaluée sur *(10 pts)*.
* Comme il a été expliqué en classe, chaque capture écran doit être commentée en respectant la numérotation du devis.
* Les noms des machines et du domaine ne doivent pas être différents de ceux du devis.
* Une pénalité de retard de 10 % pour chaque journée additionnelle de remise du travail.
* La date de remise du laboratoire est : **19 septembre 2024** avant **23h 59mn**.