## Etat des lieux :

### Utilisateur et machine :

On dispose d’un Pc principale, le « Master 2019 ». Sur celui-ci 3 Machines virtuelles (VM) sont retrouvées :

Une image contenant texte, capture d’écran, Police, logiciel

Description générée automatiquement

Une Vm sous Debian, une Vm Windows 10 permettant d’accéder à l’utilisateur Pierre Morin

Et un Windows Server servant de Domain Master sur le Lan-Abstergo dont les 3 Vm font parties.

On peut le vérifier par une commande PowerShell :

Ce serveur possède les services suivant :

Active Directory, Server Web IIS, DNS, DHCP et WSUS

On retrouve 2 Utilisateurs du réseau Lan-Abstergo :

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

L’administrateur du réseau qui s’apparenterais au Serveur Windows, L’invité est un utilisateur par défaut créer par le système mais est désactivés, krbtgt est un utilisateur built-in de l’active-directory et nous permettra d’ajouter un système d’authentification.

Le second « vrai » utilisateur est pmorin qui correspond à Pierre Morin un utilisateur du groupe comptabilité créer spécialement pour en vérifier les problèmes remonté.

Le Windows server possède tous les rôles FSMO (Maitre d’opération) :

Une image contenant texte, capture d’écran, Police, logiciel

Description générée automatiquement

SchemaMaster; DomainNamingMaster; PDCEmulator; RIDMaster; InfrastructureMaster.

Tous les informations des utilisateurs peuvent être trouvé via une commande Powershell disponible avec l’AD :

Une image contenant texte, capture d’écran, logiciel

Description générée automatiquement

On peut voir dans la catégorie « DistinguishedName » 3 types : DC ; CN ; OU

DC : Domain Components serait les branches les plus hautes de l’arbre (niveau domaine)

Ou : Organizational Units qui servent à stocker des objets (users, groups,)

CN : Common Name nom commun de l’objet (ex : pour l’utilisateur Pierre Morin, CN Pierre Morin

### Problème Aperçue :

Accès au Login d’une page web via la Vm principale mais rien ne semble s’afficher :

Une image contenant capture d’écran, logiciel, texte, Système d’exploitation

Description générée automatiquement

En fouillant dans les propriétés de la page web on parvient à afficher ceci :

Une image contenant capture d’écran, logiciel, texte, Icône d’ordinateur

Description générée automatiquement

Mais rien ne semble fonctionner en plus.

La configuration du pare-feu semble défaillante, lorsqu’un premier scan est lancé seul quelque port sont ouvert, lorsqu’une action est effectuée par exemple : Ouverture d’un site, de nouveau port sont ouvert, en revanche lorsque ce site est fermé les ports resté ouvert et sont exposé à l’extérieur.

En toute logique ils devraient se refermé après utilisation.

Une image contenant texte, capture d’écran

Description générée automatiquement

Tentative de connection au site ERP Dolibarr via la machine de Pierre Morin

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

Mais impossible car le « jeton de sécurité » à expiré

### Découverte Générale :

Découverte du site suivant :

Une image contenant texte, capture d’écran, conception

Description générée automatiquement

Par une adresse fournit sur le dossier Agent2111

Une image contenant texte, capture d’écran, Police, logiciel

Description générée automatiquement

Le mots de passe trouver sur le site correspond à l’accès au fichier, cela semble problématique.

Depuis la machine Pmorin on peut accéder correctement au site interne d’abstergo

DokuWiki :

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement