Succursale 3

Démonstration 1 : Infrastructure : Routage + DMZ + VPN (10%)

VPN (Wireguard)

Créer une Machine PFSense avec une carte réseau WAN et une carte réseau LAN.

Donner l'adresse IP 192.168.3.1 pour le réseau LAN avec un DHCP dont les plages sont 192.168.3.2 à 192.168.3.254

Création d'une VM Windows 10 pour configurer le PFSense sur https//192.168.3.1

Installer le paquet Wireguard.

Lors de la création du tunnel nous devons garder le Listen Port par défaut, copier la clé publique et la donner aux autres succursales et donner l'adresse 10.10.100.3/24 à l'interface.

Ajouter une interface pour le tunnel et inscrire l'adresse du tunnel 10.10.100.3/24 à l'interface.

Ensuite nous devons créer des Peers. Ils doivent être associés au tunnel créé, nous devons entrer les Endpoints qui sont les adresses Wan des PFsenses des autres succursales, garder le port par défaut pour les Peers et utiliser la clé publique générée lors de la création du tunnel des succursales différents pour chaque Peer que l'on crée. Ajouter les Allowed IPs suivants :

192.168.1.0/24

10.10.100.1/32

192.168.2.0/24

10.10.100.2/32

192.168.4.0/24 10.10.100.4/32

Routage

Dans PFSense ajouter une passerelle pour chaque succursale avec l'interface du tunnel :

L'adresse de la passerelle pour la succursale 1 est 10.10.100.1

L'adresse de la passerelle pour la succursale 2 est 10.10.100.2

L'adresse de la passerelle pour la succursale 4 est 10.10.100.4

Il faut aussi ajouter une route statique vers les réseaux des autres succursales avec les passerelles que nous avons créé :

Une route statique vers le réseau 192.168.1.0/24

Une route statique vers le réseau 192.168.2.0/24 Une

route statique vers le réseau 192.168.4.0/24

Démonstration 2 : Active Directory + DNS (15%) AD

Linux

Ouvrir la machine fournit.

Utiliser la commande suivante pour créer le contrôleur de domaine :

$ export PATH=$PATH:/usr/local/samba/bin samba-tool domain join 0day.com DC U"0DAY\administratreur" --dns-backend=SAMBA_INTERNAL

Pour tester la réplication la commande est :

$ samba-tool drs showrepl

Démonstration 4 : Sécurité : Pare-feu, antivirus, sauvegardes, redondance des disques, surveillance (15%) Sauvegarde (Backup Exec sur Windows)

Installation de Backup Exec sur leur site officiel.

Suivre les étapes par défaut de l'assistant.

Ajouter une machine que pour sauvegarder son fichier test.txt (nous pouvons trouver la machine avec son adresse IP 192.168.4.10 ou son nom d'ordinateur s'il est dans le domaine)

Configurer le chemin vers le fichier test.txt que nous voulons sauvegarder, appliquer la sauvegarde à toutes les semaines et la faire commencer maintenant.

Nous pouvons maintenant voir le fichier test.txt de la machine 192.168.4.10 sur l'hôte.

RAID (Windows)

4 disques de 20Go ont été ajoutés à la VM Windows Serveur.

Faire un clic droit sur l'icône Windows en bas à gauche et choisir l'option gestion du disque.

Ensuite faire un clic droit sur un des 4 disques ajoutés et choisir l'option Nouveau Volume RAID5.

Lorsque l'assistant d'installation s'affiche à l'écran faire Suivant et ensuite nous pouvons ajouter les 3 autres disques que nous avons ajouté.

Suivre toutes les étapes de l'assistant et garder les options par défaut.

Antivirus

Installation de l'antivirus Malwarebytes sur leur site.

Garder les options par défaut de l'assistant.

Se connecter avec notre compte.

L'antivirus Malwarebytes est maintenant configuré.

Surveillance

Installation du logiciel Manage Engine OpManager sur leur site.

Faire la configuration par défaut.

Nous pouvons maintenant accéder au site et surveiller notre CPU, la mémoire, le disque, un service, etc.

Démonstration 5 : Stockage, virtualisation (15%)

Configuration du SAN

4 disques de 10Go ont été ajoutés sur la VM Alma.

Ils ont été configurés en deux volumes logiques avec les commandes suivantes :

$ pvcreate /dev/sdb /dev/sdc /dev/sdd /dev/sde

$ vgcreate vg-iscsi /dev/sdb /dev/sdc /dev/sdd /dev/sde

$ lvcreate -L 20G -n lun0-windows vg-iscsi

$ lvcreate -L 20G -n lun0-linux vg-iscsi

On installe le CLI pour le target iSCSI avec la commande suivante :

$ dnf install targetcli

On se connecte au client :

$ targetcli

Configuration de SAN en mode block create

block1 /dev/vg-iscsi/lun0-linux

Création du IQN avec le nom Linux create

iqn.2023-11.ca.qc.cmontmorency:Linux

Se déplacer sur le IQN créé cd iscsi/iqn.2023-

11.ca.qc.cmontmorency:linux/tpg1/

Nous avons changé l'adresse sur laquelle écoute le serveur :

delete 0.0.0.0 3260 create

192.168.3.5

Création d'une ACL pour autoriser la VM :

acls/ create iqn.VM:VM

Nous pouvons maintenant le voir sur la VM avec la commande :

$ iscsiadm -m discovery -t st -p 192.168.3.5