Succursale 4

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 192.168.4.1 pour le réseau LAN avec un DHCP dont les plages sont 192.168.4.2 à 192.168.4.254

Création d'une VM Windows 10 pour configurer le PFSense sur https//192.168.4.1

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 10.10.100.4/24 à l'interface.

Ajouter une interface pour le tunnel et inscrire l'adresse du tunnel 10.10.100.4/24 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

192.168.3.0/24 10.10.100.3/32

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 3 est 10.10.100.3

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 192.168.3.0/24

Démonstration 2 : Active Directory + DNS (15%) Client Windows

Création d'une machine Windows 10.

Aller dans les paramètres, système, Informations et choisir l'option Renommer ce PC.

Appuyer sur l'option Changer et dans le bas on doit côcher l'option Domaine et entrer notre domaine 0day.com.

Entrer un compte qui est membre du domaine.

Après le redémarrage nous sommes maintenant membre du domaine.

RODC Windows

Création d'une machine Windows Server 2016.

Appuyer sur Ajout de rôles et fonctionnalités.

Rejoindre le domaine 0day.com et appuyer sur suivant.

Ajouter le rôles Services AD DS.

Appuyer sur suivant à toutes les autres étapes et finalement appuyer sur Installer.

Aller sur Configuration des services de domaine Active Directory et sélectionner l'option Ajouter un contrôleur de domaine à un domaine existant.

Entrer le nom de domaine et faire suivant.

Côcher tous les options (les options sont DNS, GC et RODC), entrer le mot de passe de restauration des services d'annuaire.

Prendre toutes les options par défaut pour le reste et appuyer sur Installer à la fin.

Après nous devons se reconnecter au compte et nous sommes maintenant un Read Only Domain Controller.

Samba

Installer les services suivants :

$ dnf install -y samba samba-winbind samba-winbind-clients

Changer la configuration dans le fichier /etc/samba/smb.conf :

[global]

workgroup = 0DAY

security = ADS netbios name = 0DAY

realm = 0day.com idmap config * :

range = 10000-20000 template

homedir = /profils/%U.V6 winbind

use default domain = yes

Changer les lignes suivantes dans le fichier /etc/nsswitch.conf :

passwd: files sss winbind

shadow: files sss winbind

group: files sss winbind

Nous pouvons maintenant rejoindre le domaine avec la commande suivante (Nous allons devoir entrer le mot de passe du compte Administrateur) :

$ net ads join dom.local -U Administrateur

Redémarrer les services :

$ systemctl restart winbind nmb smb

LDAP

Installation de LDAP avec la commande suivante :

$ dnf install -y openldap-clients

Changer la ligne suivante dans le fichier /etc/samba/smb.conf :

ldap server require strong auth = No

Redémarrer la machine.

Nous pouvons maintenant faire une requête LDAP avec la commande suivante (Nous allons devoir entrer le mot de passe du compte Administrateur) :

$ ldapsearch -H ldap://192.168.30.3 -D "cn=Administrator,cn=Users,dc=0day,dc=com" -W -b "dc=0day,dc=com"

Joindre le domaine avec SSSD

Découvrir le domaine avec la commande suivante :

$ realm discover 0day.com

Après avoir découvrir le domaine nous pouvons le rejoindre :

$ realm join --user=administrateur 0day.com