FreeRadius + AD

Le principe est que le serveur Radius récupère les identifiants et mots de passe des utilisateurs directement depuis le serveur Active Directory grâce au protocol NTLM (NT Lan Manager)

1. Prérequis

Installation des paquet nécessaire :

```
#apt install freeradius samba krb5-user winbindd
```

Ajout de l'utilisateur de freeradius dans le groupe winbindd pour l'accès aux comptes utilisateurs de l'AD :

```
#adduser freerad winbindd_privilegied
```

2. Ajout du serveur Radius dans le domaine

Déclaration du contrôleur de domaine dans samba:
/etc/samba/smb.conf

```
workgroup = <NomDomaine>

# Security mode. Most people will want user level
# security. See security_level.txt for details.
security = ads

======== Share Definitions ========
...

winbind use default domain = no
password server = <NomFQDNControleurDeDomaine>
realm = <NomDomaine>
```

Toujours dans le même fichier, vérification des lignes suivantes dans le partage [homes] :

```
comment = Home Directories
browseable = no
writable = yes
```

Déclaration du contrôleur de domaine dans krb5 :
/etc/krb5.conf

```
<Domaine> = {
kdc = <NomFQDNControleurDomaine>
}
```

Modification du fichier nsswith.conf et ajout de “files winbind” à chaque fin de ligne:
/etc/nsswith.conf

```
passwd: files winbind
shadow: files winbind
group: files winbind
protocols: files winbind
services: files winbind
netgroup: files winbind
automount: files winbind
```

Vérification du fonctionnement du service samba :

```
#ps -ef | grep nmbd
#ps -ef | grep smbd
```

Ajout dans le domaine :

```
#net join -U <NomAdminControleurDomaine>
```

Vérification du fonctionnement du démon winbindd :

```
#ps -ef | grep winbindd
```

Tentative de connexion avec un utilisateur du domaine :

```
#wbinfo -a <Utilisateur>%<MotDePasse>
```

Une erreur survient généralement, elle est dû au serveur qui essaye de se connecter sans l’accord de l’AD.

Test du protocole NTLM :

```
#ntlm_auth --request-nt-key --domain=<NomDomaine>
--username=<Utilisateur>
```

Résultat :

```
NT_STATUS_OK : Success (0x0)
```

3. Configuration de Freeradius

/etc/freeradius/3.0/mods-available/mschap

```
with_ntdomain_hack = yes
```

Décommenter la ligne

```
ntlm_auth = "/path/to/ntlm_auth --request-nt-key
--username=%{%{Stripped-User-Name}:-%{%{User-Name}:-None}}
--challenge=%{%{mschap:Challenge}:-00}
--nt-response=%{%{mschap:NT-Response}:-00}"
```

Ajouter

```
--domain=%{mschap:NT-Domain}
```

/etc/freeradius/3.0/mods-available/eap

Dans la section `tls-config tls-common {`
Remplacer `random_file = ${certdir}/random` par `random_file = /dev/urandom`

Redémarrage du service :

```
#systemctl restart freeradius
```