

Dans le cadre de **SECURIDAY 2009**

SECURINETS



Présente

Atelier : Radius

Formateurs: 1. Amira Methni
2. Asma Dhaouadi
3. Hend Chabbouh
4. Syrine Bejaoui

1. Présentation :

Le protocole **RADIUS** (*Remote Authentication Dial-In User Service*) est un protocole d'authentification standard.

Le fonctionnement de RADIUS est basé sur un système client/serveur chargé de définir les accès d'utilisateurs distants à un réseau. Il s'agit du protocole de prédilection des fournisseurs d'accès à Internet car il est relativement standard et propose des fonctionnalités de comptabilité permettant aux FAI de facturer précisément leurs clients.

Le protocole RADIUS repose principalement sur un serveur (le serveur RADIUS), relié à une base d'identification (base de données, annuaire LDAP, etc.) et un client RADIUS, appelé **NAS** (*Network Access Server*), faisant office d'intermédiaire entre l'utilisateur final et le serveur. L'ensemble des transactions entre le client RADIUS et le serveur RADIUS est chiffré et authentifié grâce à un secret partagé.

2. Fonctionnement de RADIUS

Le fonctionnement de RADIUS est basé sur un scénario proche de celui-ci :

- Un utilisateur envoie une requête au NAS afin d'autoriser une connexion à distance ;
- Le NAS achemine la demande au serveur RADIUS ;
- Le serveur RADIUS consulte la base de données d'identification afin de connaître le type de scénario d'identification demandé pour l'utilisateur : soit le scénario actuel convient, soit une autre méthode d'identification est demandée à l'utilisateur. Le serveur RADIUS retourne ainsi une des quatre réponses suivantes :
 - **ACCEPT** : l'identification a réussi ;
 - **REJECT** : l'identification a échoué ;
 - **CHALLENGE** : le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose un « défi » ;

3. Outils utilisés :

- **FreeRADIUS**. Téléchargeable à partir du site <http://fr.freeradius.org/>. La version utilisée est 1.1.7

Remarque : Cet atelier a été réalisé sur une distribution ubuntu 8.04

4. Partie pratique :

4.1 .Installation de Freeradius et Mysql

Pour installer freeradius il suffit de taper quelques lignes dans l'invite de commandes d'ubuntu

```
# apt-get install freeradius
# apt-get install freeradius-mysql
```

Pour l'installation de MySQL :

```
# apt-get install mysql-server
# apt-get install mysql-client
```

4.2 .Configuration de FREERADIUS et de MYSQL :

▪ Création de la base de données :

- Pour créer la base de donnée radius sous mysql, on utilise la structure mysql.sql (ou db_mysql.sql) dans l'emplacement /usr/share/doc/freeradius/examples/ fourni avec les sources du programme :

```
#mysql -u root -p </usr/share/doc/freeradius/examples/mysql.sql
```

- En donnant le mot de passe "rootpass", on arrive au prompt mysql.

```
mysql>create database radius;
mysql>use radius;
```

- La base est maintenant créée avec la structure correcte.
- On crée un utilisateur radius ayant les droits sur la base de données 'radius' afin d'éviter de diffuser mon compte root.
- Ici, ça sera un utilisateur radius avec « radius » comme mot de passe.

```
#mysql -u root -p
```

- A présent, on introduit le mot de passe passroot et on tape les commandes suivantes :

```
mysql>use mysql;
mysql>INSERT INTO radcheck(Username,Attribute,op,Value) VALUES
('radius','Password','=','radius');
```

▪ Paramétrage de freeradius pour qu'il utilise mysql :

- Il est nécessaire de modifier deux fichiers :
 - o **sql.conf** qui contient les informations d'identification à la base de données.
 - o **radiusd.conf** qui contient la configuration globale du service.
- Ces fichiers de configuration se trouvent dans /etc/freeradius
- Ci-dessous, le contenu des fichiers qu'on a utilisé

S E C U R I N E T S

Club de la sécurité informatique
I N S A T

Remarque : Dans le code des deux fichiers ci-dessous, on a enlevé tous les commentaires des fichiers textes originaux et on a ajouté et modifié à partir du fichier original que les informations écrites ci-dessous

```
# fichier sql.conf
sql {
    # Database type
    # Current supported are: rlm_sql_mysql,
    rlm_sql_postgresql,
    # rlm_sql_iodbc, rlm_sql_oracle, rlm_sql_unixodbc,
    rlm_sql_freetds
    #we specified that's rlm_sql_mysql wich we will use
    driver = "rlm_sql_mysql"

    # Connection info
    server = "localhost"
    login = "radius"
    password = "radius"

    # Database table configuration
    radius_db = "radius"
    #on ne touche pas le texte original, on modifie juste
    les champs ci-          dessus
    ...
}
```

- **radius.conf** est le fichier principal de configuration de freeradius. Ce fichier contient 500 lignes au minimum, les instructions écrites ci-dessous sont celles qui nous intéressent, le reste du texte du fichier trouvé par défaut on ne le touche pas.

```
# fichier /etc/freeradius/radiusd.conf
modules {
    chap {
        authtype = CHAP
    }

    mschap {
        authtype = MS-CHAP
        use_mppe = yes
        require_encryption = yes
        require_strong = yes
    }
}

$INCLUDE ${confdir}/sql.conf #1249
$INCLUDE ${confdir}/eap.conf
}
```

```
authorize { chap
  mschap
  sql
  eap
}

authenticate { #1887
  Auth-Type CHAP {
    chap
  }

  Auth-Type MS-CHAP {
    mschap
  }
  eap
}

accounting {
  sql
}

session {
  sql
}
```

▪ **Création de la table des NAS autorisés :**

- Le service radius n'accepte que les requêtes venant de machines strictement identifiées et authentifiées.
- Cela nous emmène à remplir une liste de machines spécifique nommé clients.conf constitué d'un bloc de 4 lignes par machine connue.
- Chaque bloc contient l'adresse ip de la machine, un mot de passe "secret" pour établir une connexion avec le radius et un nom descriptif (obligatoire) pour décrire ce client.
- Ici le fichier accepte localhost pour des tests et le NAS hypothétique qui interrogera le radius et qu'il nous faudra adapter à nos besoins.

```
# clients.conf

client 127.0.0.1 {
    secret          = radiustest
    shortname       = localhost
}
client 193.25.198.194 {
    secret          = radsecret
    shortname       = nas
}
```

```
}
```

▪ **Configuration de l'authentification par EAP :**

eap.conf est un fichier qui regroupe tous les modules d'authentification EAP.

On spécifie que l'on veut utiliser EAP-MD5 (on pourra tout de même utiliser TLS si l'on veut).

```
# eap.conf
eap {

    default_eap_type = md5

    timer_expire      = 60
    ignore_unknown_eap_types = no

    md5 {
    }
    leap {
    }

    mschapv2 {
    }
}
```

▪ **L'interface web d'administration du serveur radius:**

- Il existe sur le net plusieurs applications web avancées de gestion qui sont open source et gratuites, il nous suffira donc juste d'installer apache2 et faire les configurations nécessaires dans les fichiers d'apache.

- On peut citer : daloradius (ce qu'on a utilisé), phpradadmin...

- Daloradius comporte la gestion des utilisateurs, des NAS, des rapports graphiques, de la comptabilité, de facturation et s'intègre avec le moteur Google Maps pour géo-localiser.

Remarque : La version utilisée dans cet atelier est-0.9-4, téléchargeable à partir du site <http://code.google.com/p/daloradius/downloads/list>

4.3 .Test du Radius :

- On démarre la base de données et le radius si cela n'est pas déjà fait.

```
#/etc/init.d/mysql start
```

- Attention, la base mysql doit être démarrée avant le radius.
- On teste le résultat avec la commande dont la syntaxe est :

```
Radtest user password radius-server[:port] nas-port-number secret
```

Ce qui nous donne ceci :

```
#radtest securinets club 127.0.0.1 0 radius
```

Le résultat est correct, notre utilisateur est accepté.

```
Sending Access-Request of id 199 to 127.0.0.1 port 1812
  User-Name = "securinets"
  User-Password = "club"
  NAS-IP-Address = 255.255.255.255
  NAS-Port = 0
rad_recv: Access-Accept packet from host 127.0.0.1:1812,
id=199, length=20
```

5. Bibliographie :

<http://freeradius.org/>

<http://www.pervasive-network.org/SPIP/Installation-de-freeradius-2-4>

<http://swik.net/tutorial+freeradius?recent>

http://www.nantes-wireless.org/actu/article.php3?id_article=8&artsuite=2