Huiswerk Linux: Installatie SASL

De meeste bedrijfsnetwerken worden tegenwoording beheerd door het *Windows* operating system. Voor Windows administrators kost het bijhouden van een Linux server in zijn netwerk nogal wat extra werk. Hij moet dan namelijk op de Linux machine aparte *gebruikersprofielen* (combinatie van gebruikersnaam en wachtwoord) bijhouden. De opdracht voor deze week is: installeer en configureer de *Saslauth* daemon voor communicatie met een Windows *Domain Controller* (DC).

Let op: deze opdracht gaat ervan uit dat je kunt beschikken over een werkende Domain Controller. De minimaal benodigde *roles* zijn: Active Directory en DNS

Over SASL

Simple Authentication and Security Layer (SASL) is een door de Carnegie Mellon universiteit in Pittsburg (USA) ontwikkelde methode om de echtheid van gebruikers te bepalen. Voor het versleutelen van de wachtwoorden ondersteunt de SASL software een uitgebreide reeks van methoden, waaronder MD5, CRAM-MD5, DIGEST-MD5, GSSAPI, Kerberos en SCRAM-SHA-1.

Maar wat mooier is: de SASL software kan Windows domein-logins uitvoeren. De echtheid van gebruikers wordt dan niet bepaald via de lokale */etc/passwd* en */etc/group* bestandjes, maar via de gebruikersprofielen op een *Windows Domain Controller* (DC). Het grote voordeel hiervan is dat Linux client- en server-machines naadloos in een Windows netwerk kunnen worden geplaatst, alsof het Windows machines zijn.

Het *sudo* mechanisme

Het configureren van Linux software doen we namens de *super-user*. We moeten daarom tijdelijk inloggen als Administrator.

Cygwin gebruikers

Sudo voor Cygwin gebruikers: rechts-klik op het icoon van de Cygwin terminal, en kies voor **Als administrator uitvoeren**. Nu kunnen we de Cyrus SASL software installeren. Ook hebben we de LDAP tools nodig. Dit doen we met het volgende commando:

```
apt-get install cyrus-sasl openldap
```

Andere Linux gebruikers

Sudo voor gebruikers van andere Linux-versies (*Ubuntu*, *Lubuntu*, *Android*, *Debian, UberStudent*, etc): start een terminal met de toetsencombinatie **<Ctrl><Alt>-T**. We gebruiken het commando *sudo* om in te loggen met het *su* (become Super User) commando. Daardoor blijven we ingelogd:

```
sudo su
```

Nu kunnen we de Cyrus SASL software installeren. Dit doen we met het volgende commando:

```
apt-get install sasl2-bin ldap-utils
```

Mechanismen op de DC opvragen

Zoals bovenaan beschreven zijn er nogal wat manieren om data te versleutelen. We moeten weten welke versleutelingsmethodes door onze Domain Controller ondersteund worden. Dit kunnen we opvragen met het *ldapsearch* programma:

```
ldapsearch -H ldap://192.168.137.50 -x -s base -L supportedSASLMechanisms
```

Let op: het onderstreepte IP-adres is van mijn DC. Vervang het door het IP-adres van jouw DC.

Via optie *H* (Host) geven we aan op welk IP-adres onze DC luistert. Via optie *x* geven we aan dat we toegang willen via *simple authentication* in plaats van een volledige SASL Kerberos login. Middels optie *s* (scope) geven we aan dat niet heel de database hoeft te worden doorzocht, maar alleen de basis (*base*). We gebruiken optie *L* (LDAP format) om aan te geven welke informatie we willen zien, in dit geval de ondersteunde SASL mechanismen. De output ziet er ongeveer alsvolgt uit:

```
supportedSASLMechanisms: GSSAPI
supportedSASLMechanisms: GSS-SPNEGO
```

```
supportedSASLMechanisms: EXTERNAL
supportedSASLMechanisms: DIGEST-MD5
```

Nu weten wat we kunnen invullen in het onderstaande configuratie-bestand. We kiezen voor *DIGEST-MD5*.

De *saslauthd* configureren

De SASL software bevat onder andere het daemon-programma voor de authentificatie van gebruikers. Kijk eerst even of jouw distributie van het daemon-programma *LDAP* ondersteunt. Dit kun je opvragen middels het volgende commando:

```
saslauthd -v
```

Via de optie *v* (version) geven we aan dat we de beschikbare authentificatiemechanismen willen zien. Op mijn systeem (*Raspbian*) ziet de output er alsvolgt uit:

```
saslauthd 2.1.25
authentication mechanisms: sasldb getpwent kerberos5 pam rimap shadow ldap
```

Aanmaken configuratiebestand

Nu kunnen we de Saslauth-daemon configureren zodat hij de Windows Domain Controller kan vinden. De configuratie van de daemon wordt bijgehouden in het *saslauthd.conf* bestandje. Open het bestandje met de *vi* tekst-editor:

```
vi /etc/saslauthd.conf
```

We zien een leeg scherm. Geef het **i** (insert) commando om naar de *INSERT* modus te gaan. Geef vervolgens de onderstaande regels in:

```
ldap_servers: ldap://192.168.137.50
ldap_use_sasl: yes
ldap_mech: DIGEST-MD5
ldap_start_tls: no
```

Let op: *192.168.137.50* is het IP-adres van mijn DC. Vul hier het adres van je eigen DC in.

Middels de optie *ldap_use_sasl* geven we aan dat we de SASL mechanismen willen gebruiken voor het versleutelen van de wachtwoorden. Via optie *ldap_mech* geven we aan dat we de *DIGEST-MD5* methode willen gebruiken voor de vesleuteling van de wachtwoorden. Met de optie *ldap_start_tls* geven we aan dat de *verbinding* niet versleuteld moet worden.

Toets **<Esc>** om uit de *INSERT* mode te komen en geef de commando's *w* (write) en *q* (quit):

```
:wq
```

Het bestand wordt nu opgeslagen en je bent weer terug op de Linux command-line.

Het hoera-moment

Allereerst starten we de daemon, zodat hij gaat luisteren naar binnenkomende verzoeken om authentificatie.

Cygwin gebruikers

Nu kunnen we de daemon starten met het speciale Windows commando *net* (network):

```
service saslauth start
```

Andere Linux gebruikers

Gebruikers van andere Linux distributies, zoals *Ubuntu*, *Debian*, *Elementary*, *OSX*, etc. starten de Saslauth daemon alsvolgt:

```
service saslauthd start
```

We kunnen nu testen of het werkt. Dit doen we met het programma *testsaslauthd*:

```
testsaslauthd -u testuser -p Welkom#1
```

Let op: de gebruiker en het wachtwoord zijn geldig op mijn eigen *Domain Controller*. Gebruik login-gegevens welke op jouw DC geldig zijn. De *Admninistrator* gebruiker mag/werkt niet. Maak een aparte test-gebruiker aan. Bij een succesvolle login kun je de volgende output zien:

```
0: OK "Success."
```

Huiswerk opsturen

Zoals je inmiddels weet, kun je de opdracht aftekenen door een e-mail met daarin de output van het *history* commando te versturen. Dit doen we met een pijpleiding tussen de commando's *history* en *email*. Zorg dat het onderwerp van de e-mail tussen aanhalingstekens staat:

```
history | email -s "SASL installatie" docent@localhost
```

Als je geen foutmelding ziet is de e-mail succesvol verstuurd.

Administrator uitloggen

We hebben de saslauth daemon geïnstalleerd en geconfigureerd zodat we kunnen communiceren met een Windows Domain Controller, maar we zijn nog steeds ingelogd als Administrator (*root*).

Geef tot slot **<Ctrl>-D** om de Administrator uit te loggen.

Problemen oplossen

Het kan zijn dat je tijdens het starten de volgende waarschuwing krijgt:

```
[warn] To enable saslauthd, edit /etc/default/saslauthd and set START=yes ... (warning).
```

Open dan het genoemde bestand met de *vi* editor:

```
vi /etc/default/saslauthd
```

Geef het *vi* commando i (insert) en wijzig vervolgens de vetgedrukte instellingen:

```
# Should saslauthd run automatically on startup? (default: no)
START=yes

# Example: MECHANISMS="pam"
MECHANISMS="ldap"
```

Omdat wij willen communiceren met een *Domain Controller*, zetten wij de instelling voor MECHANISMS op *ldap* (Lightweight Database Access Protocol).

Toets **<Esc>** om uit de *INSERT* modus te komen en geef de commando's *w* (write) en *q* (quit):

```
:wq
```

Het configuratie-bestand wordt dan opgeslagen en we zijn terug op de commando prompt.