WLAN-Anmeldung über Radiusserver

in diesem Tutorial soll beschrieben werden, wie man Zugänge zu WLANs per radius absichern kann

Installation

```
aptitude install freeradius
```

Konfiguration

Alle Konfigurationsdateien befinden sich im Verzeichnis `/etc/freeradius`

Gerätekonfiguration

Zunächst muss man dem Radius erklären, welcher WLAN Zugangspunkt überhaupt zugriff gewährt werden soll. Dies geschieht in der Datei `clients.conf`. Die IP-Adressen können separat (192.168.0.100/32)oder als ganzes Netz (192.168.0.0/24) eingegeben werden.

```
client 192.168.0.0/24 {
        secret          = testing123
        shortname       = WLAN-test
}
```

Dieser Eintrag gewährt allen WLAN Zugrangspunkten mit der Adresse 192.168.0.x Zugang zum Radiusserver. Die Kommunikation von Radius und Accesspoint wird per Passwort abgesichert. Dieses Kennwort wird unter Secret angegeben.

Sollten mehrere AccessPoints verwendet werden, kann man diese auch mit separaten Kennworten ansprechen.

```
client ap1 {
        ipaddr = 192.168.0.20
        netmask = 32
        secret = testing_ap1
}

client ap2 {
        ipaddr = 192.168.0.21
        netmask = 32
        secret = testing_ap2
```

```
}
```

Userkonfiguration

Als nächstes sollte man sich die Datei `users.conf` zu gemüte führen. In dieser Datei sind alle Usernamen und Passwörter abgelegt, die der Accesspoint entgegen nimmt. Auch Anmeldezeiten und andere nützliche Dinge können hier hinterlegt werden.

```
"User1"       Cleartext-Passwort := "Geheim"
"User2"       Cleartext-Passwort := "Geheim", Login-Time := "wk0700-1800"
"User3"       Cleartext-Passwort := "Geheim", Login-Time :="A1000-1700"
```

Alle User haben das Passwort geheim. Der User2 kann sich aber nur wochentags von 7:00 - 18:00 anmelden, der User3 an allen Tagen von 10:00 - 17:00. Weitere Attribute findet man unter http://freeradius.org/rfc/attributes.html

Zertifikate

Als nächstes muss man die Zertifikate erzeugen, mit denen das am Laptop eingegebene Passwort sicher zum AccessPoint übertragen werden soll. Dazu muss man ins Verzeichnis `/etc/freeradius/certs` wechseln und alle unnötigen Dateien löschen

```
rm -f *.pem *.der *.csr *.crt *.key *.p12 serial* index.txt*
```

Als zweiten Schritt kopiert man sich den Inhalt des Verzeichnises `/usr/share/doc/freeradius/examples/certs/` in das Verzeichnis `/etc/freeradius/certs/` und wechselt in dieses. In diesem Verzeichnis befindet sich nun eine Beispielkonfiguration, die man nach eigenen Wünschen anpassen kann.

Zertifikate generieren

Die Datei ca.cnf stellt die Einstellungen für die Certification Authority dar. Folgende Inhalte sollten nach eigene Wünschen angepasst werden:

```
[ CA_default ]
default_days            = 3650

[ req ]
input_password          = testing123
output_password         = testing123

[certificate_authority]
countryName             = DE
stateOrProvinceName     = Radius
```

```
localityName            = Bad Neustadt / Saale
organizationName        = da-checka.de
emailAddress            = patrick.schindelmann@googlemail.com
commonName              = "radiustest"
```

Die gleichen Einstellungen sollte man auch in der Datei `server.cnf` eintragen. Vor allem das Passwort sollte gleich sein.

Zur Zertifikatserstellung führt man in dem Verzeichnis `certs` das Kommando

```
make all
```

aus. Alle benötigten Dateien werden in dem Verzeichnis erzeugt. Die Datei `ca.der` sollte man sich auf einen USB-Stick sichern, da diese bei jedem Rechner benötigt wird, der sich am AccessPoint anmelden soll.

Zertifikatsbenutzung

Da das Zertifikat mit einem Passwort (testing123) gesichert ist, muss man freeradius dazu bringen, dieses Passwort beim lesen des Zertifikats zu nutzen. Dazu muss in der Datei `eap.conf` der Eintrag private_key_password gesucht und der Wert „whatever“ in „testing123“ geändertt werden.

Radius testen

Zunächst sollte man sich das Radius Log-file unter `/var/log/freeradius/radius.log` anschauen. Sollten dies zu wenige Informationen sein, muss man den Radius-Server stoppen und im Debug-Modus starten.

```
/etc/init.d/freeradius stop
freeradius -X
```

Das Paket radius-utils enthält das sehr nützliche Programm radtest. Mit diesem Werkzeug kann man die Passwortkonfigurationen testen. Benutzt wird es wie folgt:

```
radtest <Username> <Userpasswort> <RadiusserverIP> <Port> <Gerätepasswort>
```

In meinem Fall baut sich der Befehlt wie folgt auf

```
radtest Patrick Geheim 127.0.0.1 1812 testing123
```

AccessPoint vorbereiten

Im AccessPoint muss der Verschlüsselungsalgorithmus auf WPA2-Enterprise gestellt werden.

Weiterhin muss die IP und der Port des Radiusservers eingetragen werden, sowie das oben definierte Paswort (testing123).

Fertig

Windows einrichten

Zunächst sollte man sich die Datei `ca.der` vom Radiusserver (im Verzeichnis `/etc/freeradius/cert` auf einen USB-Stick kopieren. Diese ist das Zertifikat, das die verschlüsselte Passwortübermittlung vom Client zum AccessPoint sicherstellt.

Auf dem Client muss dieses Installiert werden. Auf Windows XP Systemen muss man den Assistenten nur durchklicken. Bei Windows 7 und 8 muss man den Zertifikatsspeicher manuell auf „Vertrauenswürdige Stammzertifizierungsstellen“ setzen.

Jetzt muss noch ein Profil für das WLAN erzeugen. In einem Profil stehen alle Daten, die für eine Authentifizierung wichtig sind:

- AccessPoint Name / SSID
- passendes Zertifikat
- Verchlüsselungsalgorithmus

Quellen

- http://www.heise.de/netze/artikel/WLAN-sichern-mit-Radius-1075339.html
- http://www.tecchannel.de/netzwerk/wlan/2036067/workshop_freeradius_fuer_linux_einrichten/index.html
- http://www.wi-fiplanet.com/tutorials/article.php/3557251/FreeRADIUS-and-Linux-for-Your-WLAN.htm
- http://kupschke.net/2012/04/16/freeradius-mit-eap-ttls-und-ldap-zur-sicheren-wlan-authentifizierung/
- http://www.administrator.de/wissen/sichere-wlan-benutzer-authentifizierung-%C3%BCber-radius-142241.html

From:
https://wiki.da-checka.de/ - **PSwiki**

Permanent link:
https://wiki.da-checka.de/doku.php/wiki/sicherheit/wlan_mit_radius?rev=1364028233

Last update: **2013/03/23 09:43**