Eapol test

eapol_test

Viene con el wpa_supplicant de Linux pero por ejemplo en el paquete de Debian no viene y por lo tanto hay que compilarlo a mano. Con él podremos simular las connexiones soportadas en Eduroam:

- TTLS + MSCHAPv2
- PEAP + MSCHAPv2
- TTLS + PAP

Pasos para compilarlo:

Descargar el wpa_supplicant y ejecutar:

```
$ cd wpa_supplicant-version
$ cat defconfig | sed -e 's/#CONFIG_EAPOL_TEST=/CONFIG_EAPOL_TEST=/' > .config
$ make eapol_test
```

Copy paste del siguiente código que nos creará dos ficheros ttls_pap.conf, peap_mschapv2.conf Y ttls_mschap.conf

```
$ cat > ttls_pap.conf << EOF
 network={
 ssid="eduroam"
 scan_ssid=1
 key_mgmt=WPA-EAP
 eap=TTLS
 identity="usuario@dominio.tld"
 anonymous_identity="anonimo@dominio.tld"
 password="secret"
 phase2="auth=PAP"
 ca_cert="/path/certificado/GlobalSignRoot.der"
# Para comprobar el nombre del servidor de Radius (nombre que ofrece el certificado)
 subject_match="/C=GB/L=York/O=University of York/OU=Computing Service/OU=Terms of use at www.verisign.co.uk
/rpa (c)05/OU=Authenticated by VeriSign/OU=Member, VeriSign Trust Network/CN=nasaaa1.york.ac.uk"
 }
 EOF

$ cat > peap_mschapv2.conf << EOF
# La inner y la outer deben ser la misma y deben ser validas
 network={
 ssid="eduroam"
 scan_ssid=1
 eap=PEAP
 eapol_flags=0
 key_mgmt=WPA-EAP
 identity="usuario@dominio.tld"
 password="secret"
 ca_cert="/path/certificados/GlobalSignRoot.der"
 phase1="peapver=0"
 phase2="auth=MSCHAPV2"
 anonymous_identity="usuario@dominio.tld"
# Para comprobar el nombre del servidor de Radius (nombre que ofrece el certificado)
 subject_match="/C=GB/L=York/O=University of York/OU=Computing Service/OU=Terms of use at www.verisign.co.uk
/rpa (c)05/OU=Authenticated by VeriSign/OU=Member, VeriSign Trust Network/CN=nasaaa1.york.ac.uk"
 }
 EOF

cat > ttls_mschap.conf << EOF
 network={
 eap=PEAP
 eapol_flags=0
 key_mgmt=WPA-EAP
 identity="usuario@dominio.tld"
 password="secret"
 anonymous_identity="usuario@dominio.tld"
 ca_cert="/path/certificado/GlobalSignRoot.der"
 phase1="peapver=0"
 phase2="auth=MSCHAPV2"
# Para comprobar el nombre del servidor de Radius (nombre que ofrece el certificado)
 subject_match="/C=GB/L=York/O=University of York/OU=Computing Service/OU=Terms of use at www.verisign.co.uk
/rpa (c)05/OU=Authenticated by VeriSign/OU=Member, VeriSign Trust Network/CN=nasaaa1.york.ac.uk"
 }
 EOF
```

Tendremos que cambiar el usuario y la contraseña por unos que sean válidos. El inner i el outer cuando se utiliza MSCAHPv2 tienen que ser el mismo. Lo ejecutamos así:

```
$ ./eapol_test -c ttls_pap.conf -a RADIUS -s SECRETO
$ ./eapol_test -c peap_mschapv2.conf -a RADIUS -s SECRETO
$ ./eapol_test -c ttls_mschapv2.conf -a RADIUS -s SECRETO
```

Nos sacará un chorro de información y si termina bien dirá SUCCES, de lo contrarió terminará con un FAILURE.