FreeRADIUS + OpenLDAP with SASL

When using FreeRADIUS with LDAP passthrough authentication, such as OpenLDAP with SASL or Kerberos passthrough, you are very restricted in what you can do.

DeployingRADIUS, Alan DeKok's site, has a handy compatibility matrix that lists authentication systems and their authentication protocol compatibility. LDAP servers with passthrough authentication require you to bind to LDAP as the user, which in the compatibility matrix limits you to PAP authentication and its EAP variations (such as EAP-TTLS/PAP and EAP-TTLS/EAP-GTC with PAP).

Step-by-step guide

1. Modify FreeRADIUS LDAP support

1. Install the freeradius-ldap module, if you haven't already.
2. Configure the `ldap` module as per the standard configuration with the server name(s), port(s), and whether TLS is required.
3. Below the `base_dn`, from which all searches start, you will find the `update` section, which returns attributes from LDAP. This may include the `user Password` LDAP attribute, which FreeRADIUS will use to authenticate. Since you will use bind-as-user, this is not required. Comment it out.
4. Scroll to the `user` section. You may wish to modify the `base_dn`, `filter`, and `scope` settings there to match what your LDAP requires to return a single user object. FreeRADIUS will set an `Ldap-UserDN` attribute that will be used for binding as a user if the search is successful.

   > You may wish to test your LDAP search with tools such as `ldapsearch` to test your DN and your filters. See http://wiki.freeradius.org/modules/Rlm_ldap for more information.

5. Save the file.

2. Modify FreeRADIUS authentication support

> It is assumed here that you will modify the `inner-tunnel` site as Moonshot will use EAP-TTLS, and set the default EAP type in the `ttls` section to `gtc` for PAP support.

1. Insert into the bottom of the `authorize` section after the `pap` line the following:

```
if (User-Password) {
        update control {
                Auth-Type := ldap
        }
}
```

2. In the `authenticate` section, modify the `Auth-Type PAP` option as shown below:

```
Auth-Type PAP {
        # pap
        ldap
}
```

3. Additionally, remove the comment from the `ldap` line in the `Auth-Type LDAP` block, but not the block itself.
4. Save the file.

3. Modify FreeRADIUS EAP support

It is rare that network access servers still use PAP. Instead, they use a variety of EAP types, which can wrap PAP to provide better security for user credentials.

Since bind-as-user is limited to PAP, you are limited to EAP-GTC (which has PAP support).

The default settings in the `eap` module in FreeRADIUS set PAP as the password mechanism for EAP-GTC, so no changes are required. What is required though is setting the default type for EAP conversations:

1. If you intend to use just EAP-GTC without any further tunnelling, set the first instance of `default_eap_type` to `gtc`.
2. To set the default EAP type in tunneled EAP conversations, such as EAP-TTLS, scroll to the `ttls` section, then set its `default_eap_type` to `gt` .

PEAP support also includes a `default_eap_type` setting.

If you are using Cisco's PEAPv1, which supports EAP-GTC, you can set that `default_eap_type` to `gtc`.

If you are using Microsoft's PEAPv0, the `default_eap_type` must remain `mschapv2` (the default).