LDAPTLS_REQCERT=never ldapsearch -H ldaps://miservidor.midominio.local -LLL -b "dc=midominio,dc=local"

NOTA: Para comprobar que efectivament la consulta se ha hecho con el usuario que adquierió el TGT (usu1ldap) se puede ejecutar *LDAPTLS_REQCERT=never ldapwhoami -H ldaps://miservidor.midominio.local*

NOTA: Note that in Kerberos, authentication is always mutual. This means that not only have you authenticated yourself to the LDAP server, but also the LDAP server has authenticated itself to you. In particular, this means communication is with the desired LDAP server, rather than some bogus service set up by an attacker.

*Configuració de l'inici de sessió fent servir Kerberos/LDAP:

Un cop ja hem comprovat que la "coordinació" entre el servidor Kerberos i el servidor LDAP funciona si es demana des de la nostra màquina client, ara només caldrà indicar al servidor SSSD d'aquesta darrera que faci ús d'aquells dos servidors que ja treballen plegats. Concretament haurem de modificar el fitxer de configuració "/etc/sssd/sssd.conf" per a què tingui un contingut similar al següent (i seguidament reiniciar el servei SSSD):

```
[sssd]
domains=pepito
[domain/pepito]
auth_provider=krb5
krb5_server=kdc.midominio.local
krb5_realm=MIDOMINIO.LOCAL
id_provider=ldap
ldap_uri=ldaps://miservidor.midominio.local
ldap_search_base=dc=midominio,dc=local
ldap_tls_reqcert=allow
ldap_id_use_start_tls = true
ldap_sasl_mech = gss-spnego  #Indica la llibreria que usarà el client per enviar el TGS al LDAP
ldap_sasl_authid = host/client.midominio.local@MIDOMINIO.LOCAL
```

I ja està: a partir d'aquí, un cop l'usuari inicïi sessió (via gdm, *su -l usu1ldap*, etc) escrivint la seva contrasenya, obtindrà automàticament un TGT que farà servir tot seguit per demanar al KDC un TGS per fer-lo servir contra el servidor LDAP (concretament, per realitzar una consulta autenticada mitjançant la llibreria GSS-SPNEGO, que forma part del "framework" de seguretat SASL), obtenint així (sense haver-se d'autenticar de nou) la resta de dades identificatives que necessita per iniciar sessió.