mod05_ex03: Reviewing Plugable Authentication Modules

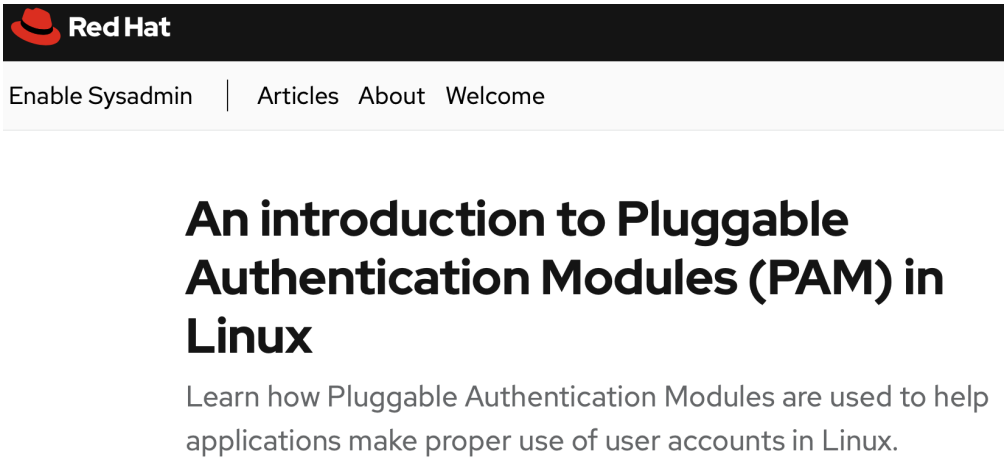
The purpose of this exercise is to introduce Plugable Authenticaition Modules (PAM) and to overview the supporting files. The exercise also provides future reading assignments to enhance your knowledge and skills in configuring PAM.

Reference Information

- PAM Modules: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/5/html/deployment_guide/s1-pam-format
- SSSD: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/5/html/deployment_guide/sssd
- LDAP: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/5/html/deployment_guide/ch-ldap

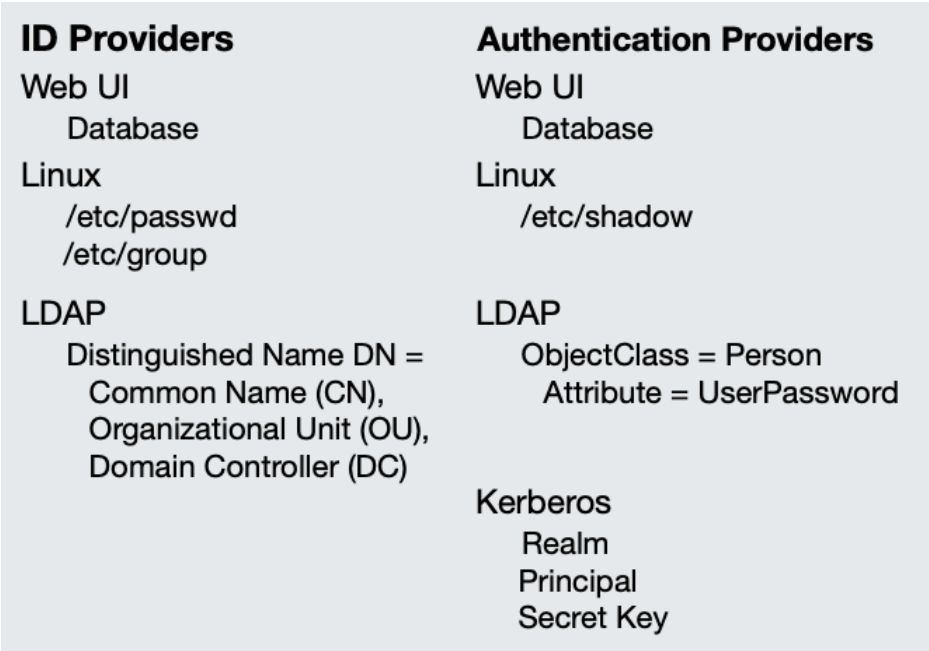
1. Understanding Plugable Authentication Modules (PAM).

1.1 Begin this exercise by reading a RedHat article overviewing Pluggable Authentication Modules (PAM).

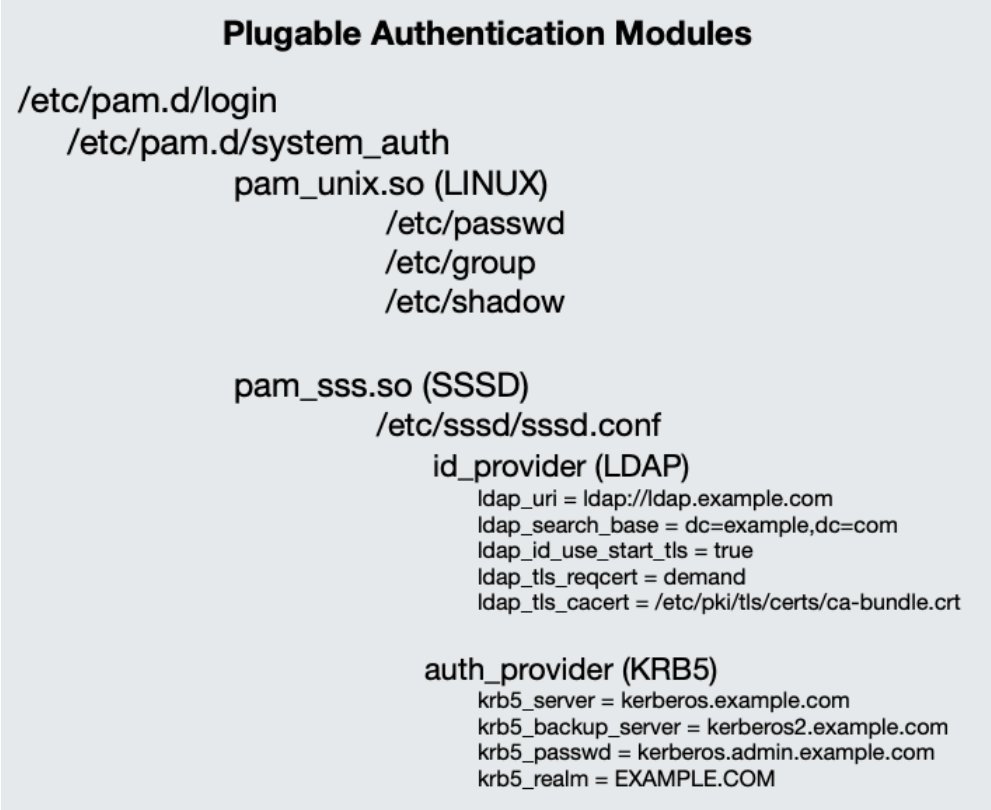


https://www.redhat.com/sysadmin/pluggable-authentication-modules-pam

1.2 An identity provider acknowledges the User ID. The authentication provider validates the user's password. For local users CDP uses /etc/passwd for the identity provider and /etc/shadow for the authentication provider. For Directory Services CDP uses LDAP for the identity provider and Kerberos for the authentication provider.

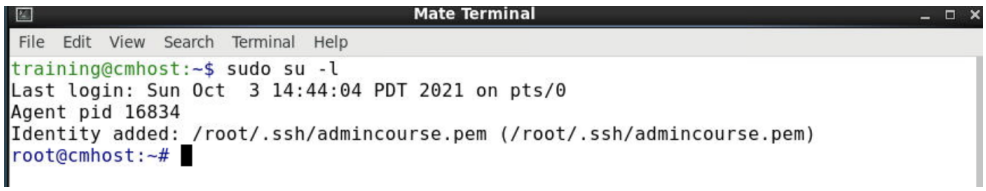


1.3 CDP uses Plugable Authentication Modules to connect to both Linux files and to System Security Service Daemon (SSSD). The key configuration file is /etc/sssd/sssd.conf, which provides the connection strings to LDAP and to Kerberos.



2. Open a Mate terminal as the local administrative user, training.

2.1 Open a Mate terminal. Use the sudo command to become the root user.




```
% sudo su -l
```

3. Reviewed the shared object files which are the actual Pluggable Authentication Modules.

3.1 Change directory to /usr/lib64/security.

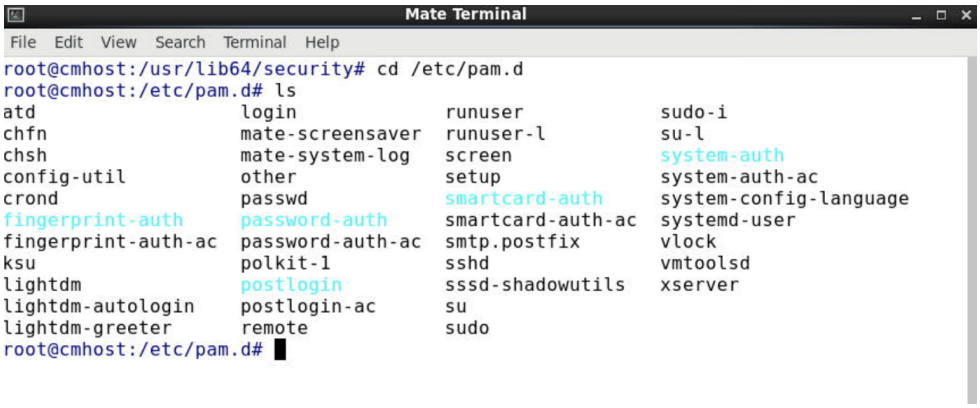

```
# cd /usr/lib64/security
```

3.2 List the contents. Review the list of PAM modules. Notice pam_unix.so and pam_sss.so. These are shared object files that control access to Unix and to SSSD.


```
# ls
```

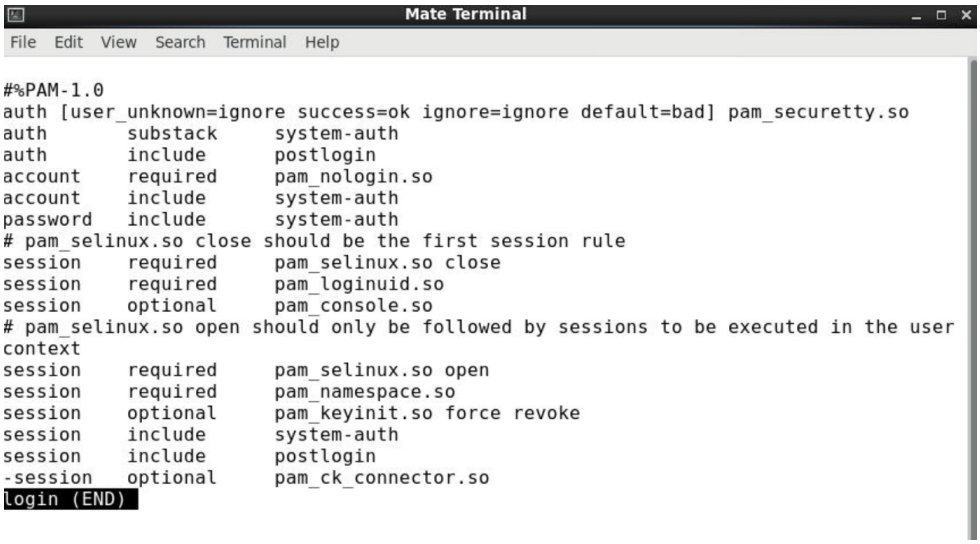
4. Review /etc/pam.d/login file.

4.1 Change directory to /etc/pam.d. List the contents. The pam.d directory contains the PAM configuration files for each PAM-aware application. The configuration files names are intended to be self-explanatory.




```
# cd /etc/pam.d
# ls
```

4.2 Use the less command to display the login file.




```
# less login
```

The PAM configuration files have standard fields for each line.

- <module interface> account
- <control_flag> required
- <module_name> pam_nologin.so
- <module_arguments>

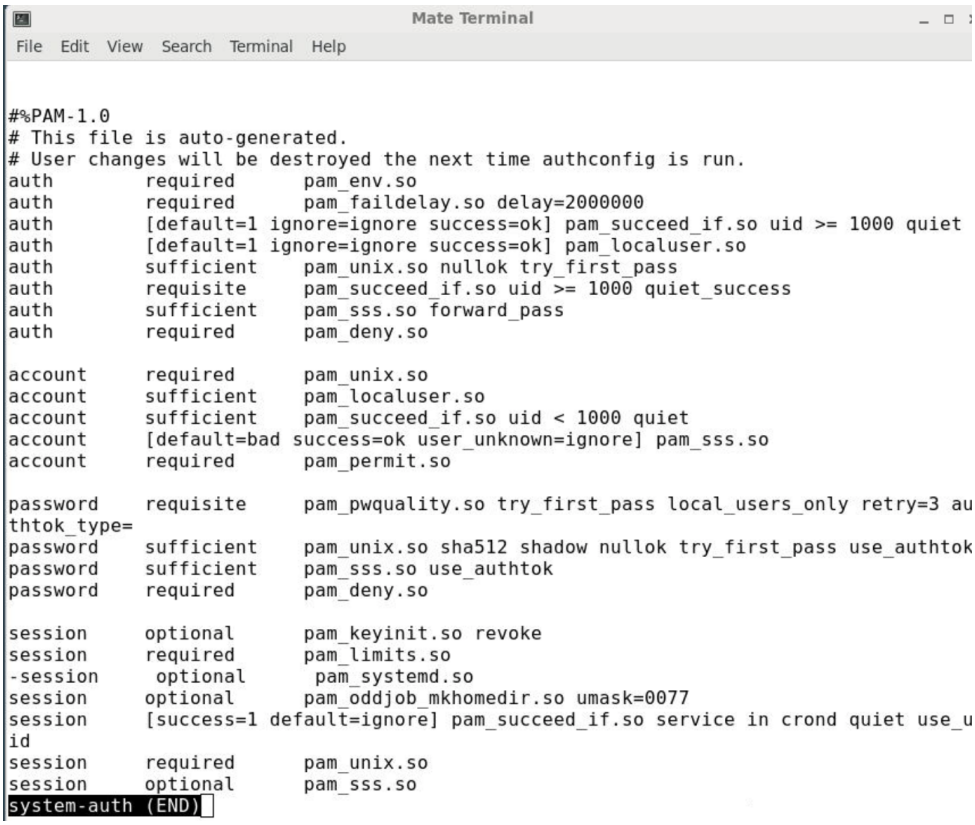
4.3 There are four types of PAM interfaces.

- **auth** provides the interface to the authentication mechanism
- **account** provides the rules for allowing the authentication
- **password** for changing user passwords
- **session** manages the user sessions

4.4 Notice that the auth, account, and session module interfaces are pointing to another configuration file, system-auth. Quit the login configuration file.

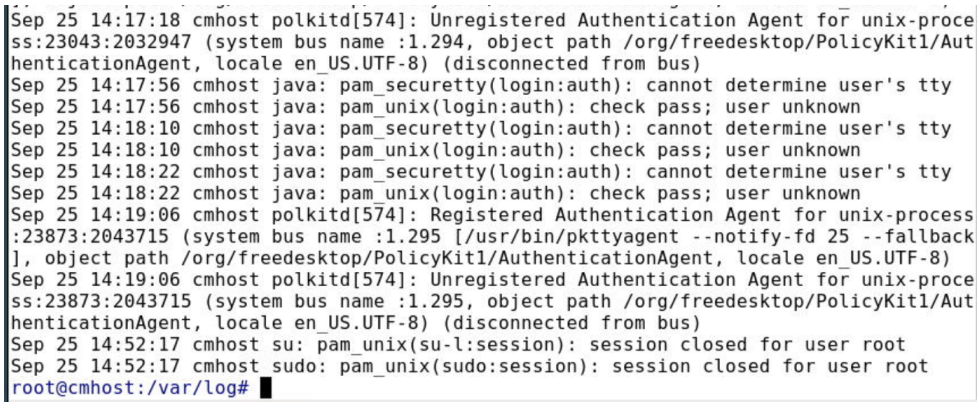
5. Review /etc/pam.d/system-auth file.

5.1 Use the less command to display the system-auth file. The two important configurations in the system-auth file are the auth, account, password, and session module interfaces that are pointing to the PAM modules pam_unix.so and pam_sss.so. PAM authentication works in order of listing, so first the local Linux files will be checked and then the authentication will be passed to SSSD. Quit the less command.




```
# less system-auth
```

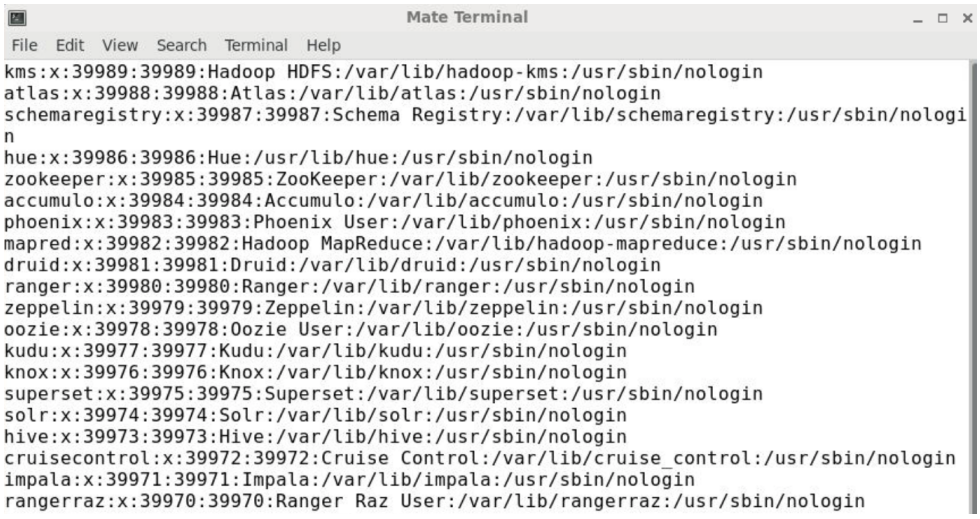
5.2 Use the less command to display the log file for PAM, /var/log/secure. The PAM log file is detailed. It should be the first place to review when troubleshooting. Here you can see a log tail for a login attempt from an user that can not be identified.




```
# less /var/log/secure
```

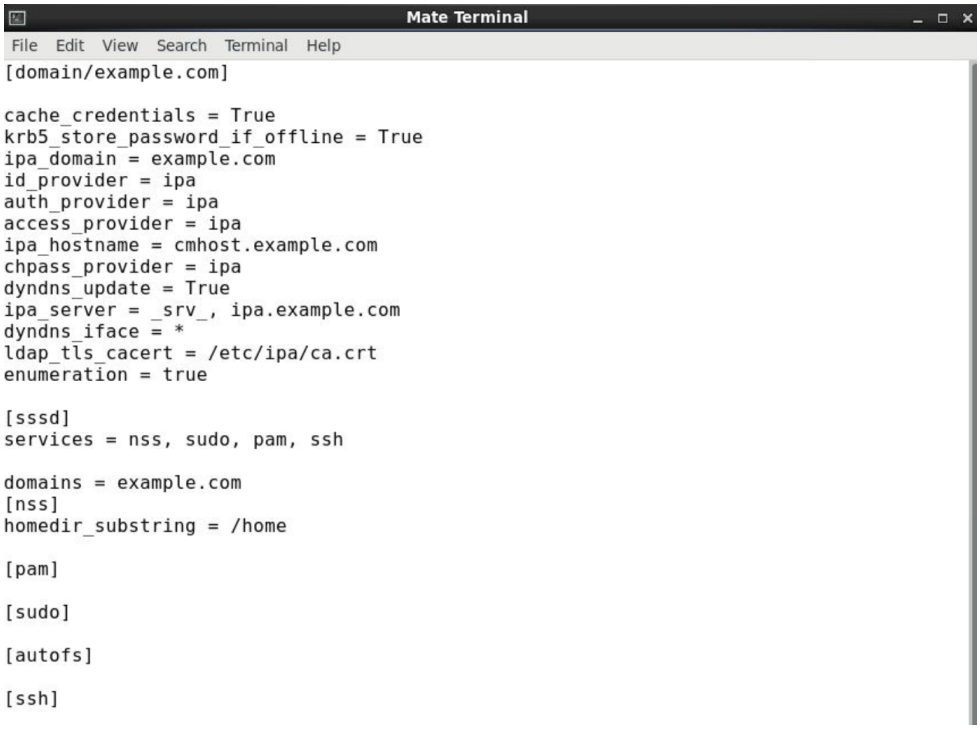
6. Review /etc/passwd and /etc/sssd/sssd.conf.

6.1 Use the less command to display the contents of the /etc/passwd file. The PAM module unix.so will access and manage /etc/passwd, /etc/group, and /etc/shadow. All of these users will be able to authenticate. Note that all CDP service accounts do not allow direct login. Quit the less command.




```
# less /etc/passwd
```

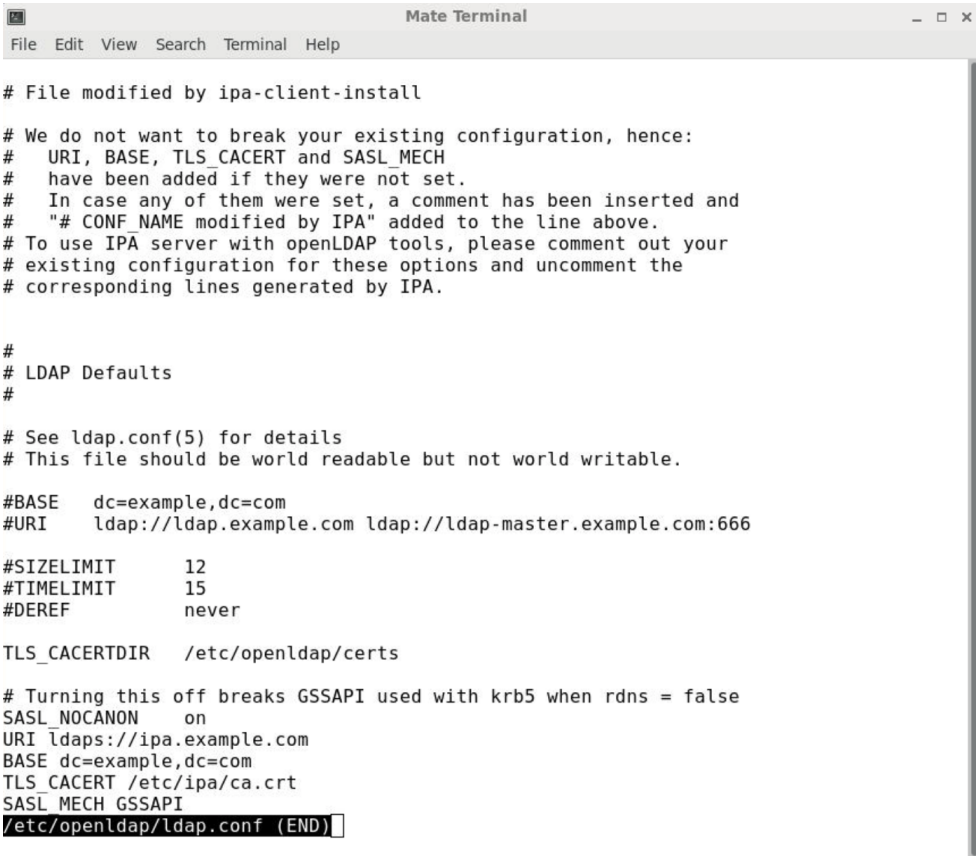
6.2 Use the less command to display the /etc/sssd/sssd.conf file. The PAM module for pam_sss.so accesses the /etc/sssd/sssd.conf file. This file has properties for an id_provider = ipa and an access_provider = ipa. This is because we are using the ipa client. In actuallty the id_provider is LDAP and the access_provider is Kerberos. Quit the less command.




```
# less /etc/sssd/sssd.conf
```

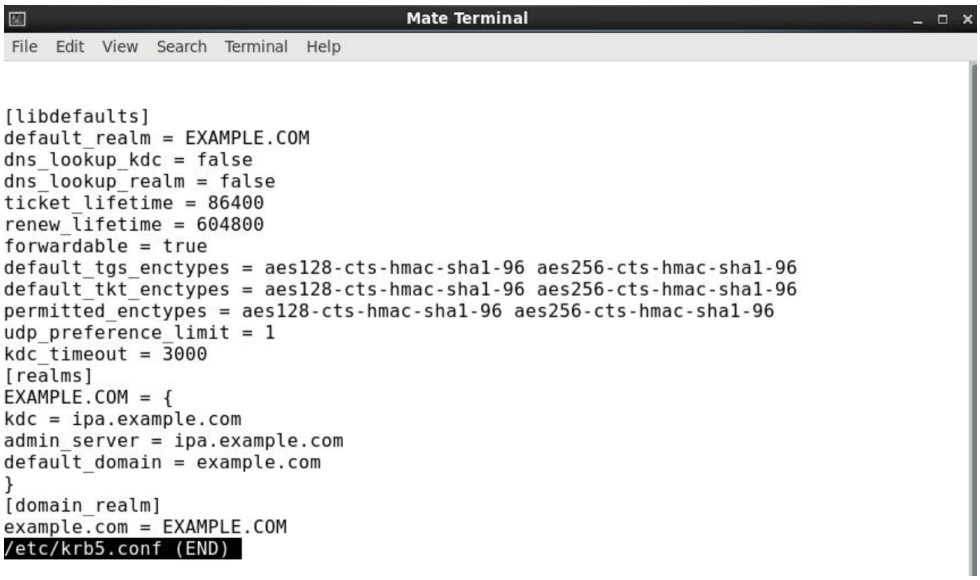
7. Review other files.

7.1 Use the less command to display the /etc/openldap/ldap.conf file. The properties of URI, BASE, TLS_CACERT, and SASL_MECH define how to connect to LDAP. This is a secure ldaps connection. Quit the less command.



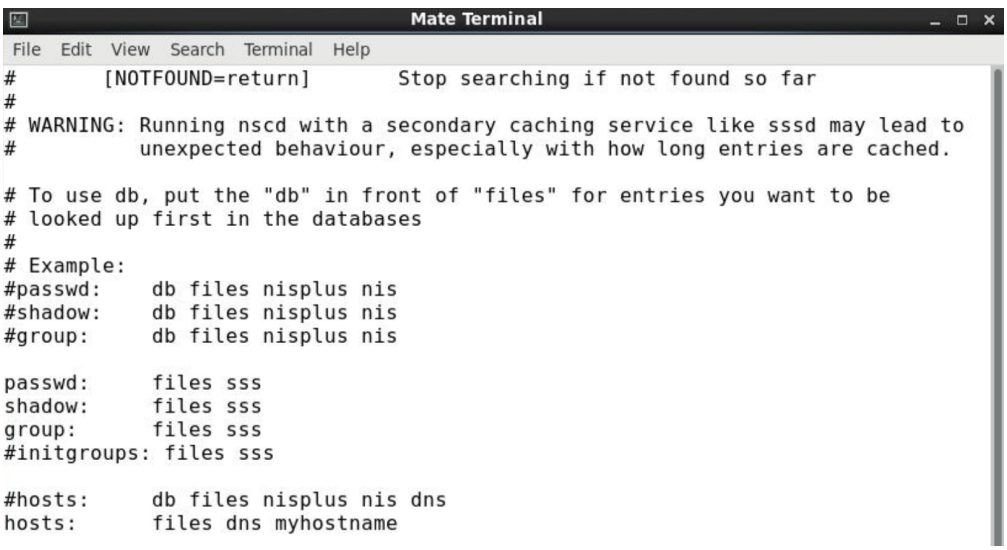

```
# less /etc/openldap/ldap.conf
```

7.2 Use the less command to display the /etc/krb5.conf file. This properties of default_realm, kdc, admin_server, and default_domain define the connection to the Kerberos Key Distribution Center (KDC). Quit the less command.




```
# less /etc/krb5.conf
```

7.3 Use the less command to display the /etc/nsswitch.conf file. The Name Service Switch (NSS) is a look up service for name resolution. It can point to a number of different common configuration databases. These include Linux files, DNS, NIS, and SSSD. This configuration points first to Linux files (/etc/passwd,/etc/group,/etc/shadow) and then to SSSD.




```
# less /etc/nsswitch.conf
```

7.4 Exit back to the user training.

8. Mastering the PAM architecture and tools takes research and practice. A good place to continue is to read RedHat documentation for PAM.