

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 Pluggable Authentication Modules (PAM).

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

The screenshot shows the Red Hat logo and navigation menu. The main title is "An introduction to Pluggable Authentication Modules (PAM) in Linux". Below it is a subtitle: "Learn how Pluggable Authentication Modules are used to help applications make proper use of user accounts in Linux."

<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.

ID Providers	Authentication Providers
Web UI	Web UI
Database	Database
Linux	Linux
/etc/passwd	/etc/shadow
/etc/group	
LDAP	LDAP
Distinguished Name DN = Common Name (CN), Organizational Unit (OU), Domain Controller (DC)	ObjectClass = Person Attribute = UserPassword
	Kerberos
	Realm
	Principal
	Secret Key

1.3 CDP uses Pluggable 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.

```
Plugable Authentication Modules

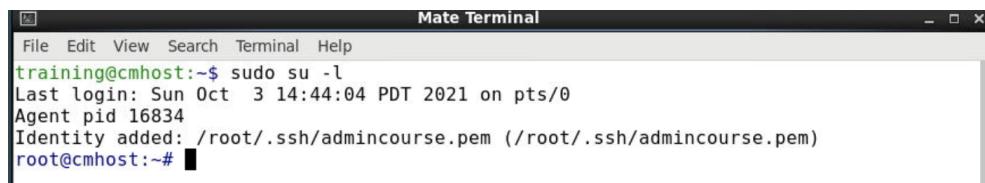
/etc/pam.d/login
/etc/pam.d/system_auth
    pam_unix.so (LINUX)
        /etc/passwd
        /etc/group
        /etc/shadow

pam_sss.so (SSSD)
/etc/sssd/sssd.conf
    id_provider (LDAP)
        ldap_uri = ldap://ldap.example.com
        ldap_search_base = dc=example,dc=com
        ldap_id_use_start_tls = true
        ldap_tls_reqcert = demand
        ldap_tls_cacert = /etc/pki/tls/certs/ca-bundle.crt

    auth_provider (KRB5)
        krb5_server = kerberos.example.com
        krb5_backup_server = kerberos2.example.com
        krb5_passwd = kerberos.admin.example.com
        krb5_realm = EXAMPLE.COM
```

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.



The screenshot shows a terminal window titled "Mate Terminal". The user "training" is logged in. The command "sudo su -l" is entered, followed by a password prompt. The terminal output shows the user switching to root and logging in, with the message "Identity added: /root/.ssh/admincourse.pem (/root/.ssh/admincourse.pem)".

```
% sudo su -l
```

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

3.1 Change directory to /usr/lib64/security.



```
Mate Terminal
File Edit View Search Terminal Help
root@cmhost:~# cd /usr/lib64/security
root@cmhost:/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.



```
Mate Terminal
File Edit View Search Terminal Help
root@cmhost:~# cd /usr/lib64/security
root@cmhost:/usr/lib64/security# ls
pam_access.so      pam_limits.so      pam_sss.so
pam_cap.so         pam_listfile.so    pam_stress.so
pam_chroot.so      pam_localuser.so  pam_succeed_if.so
pam_console.so     pam_loginuid.so   pam_systemd.so
pam_cracklib.so   pam_mail.so       pam_tally2.so
pam_debug.so        pam_mkhomedir.so pam_time.so
pam_deny.so         pam_motd.so      pam_timestamp.so
pam_echo.so         pam_namespace.so pam_tty_audit.so
pam_env.so          pam_nologin.so   pam_umask.so
pam_exec.so         pam_oddjob_mkhomedir.so pam_unix_acct.so
pam_faildelay.so   pam_permit.so    pam_unix_auth.so
pam_faillock.so    pam_postgresok.so pam_unix_passwd.so
pam_filter          pam_pwhistory.so  pam_unix_session.so
pam_filter.so       pam_pwquality.so pam_unix.so
pam_ftp.so          pam_rhosts.so    pam_userdb.so
pam_gnome_keyring.so pam_rootok.so   pam_user_map.so
pam_group.so        pam_securetty.so pam_warn.so
pam_issue.so        pam_selinux_permit.so pam_wheel.so
pam_keyinit.so     pam_selinux.so   pam_xauth.so
pam_lastlog.so     pam_sepermit.so
pam_ldap.so         pam_shells.so
```

```
# 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.

```
root@cmhost:/usr/lib64/security# cd /etc/pam.d
root@cmhost:/etc/pam.d# ls
atd           login          runuser        sudo-i
chfn          mate-screensaver runuser-l     su-l
chsh          mate-system-log screen        system-auth
config-util   other          setup         system-auth-ac
crond         passwd         smartcard-auth system-config-language
fingerprint-auth password-auth smartcard-auth-ac systemd-user
fingerprint-auth-ac password-auth-ac smtp.postfix vlock
ksu           polkit-1       sshd          vmtoolsd
lightdm       postlogin      sssd-shadowutils xserver
lightdm-autologin postlogin-ac su
lightdm-greeter remote        sudo
root@cmhost:/etc/pam.d#
```

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

4.2 Use the less command to display the login file.

```
%PAM-1.0
auth [user_unknown=ignore success=ok ignore=ignore default=bad] pam_securetty.so
auth    substack    system-auth
auth    include    postlogin
account required    pam_nologin.so
account include    system-auth
password include    system-auth
# pam_selinux.so close should be the first session rule
session required    pam_selinux.so close
session required    pam_loginuid.so
session optional    pam_console.so
# pam_selinux.so open should only be followed by sessions to be executed in the user
context
session required    pam_selinux.so open
session required    pam_namespace.so
session optional    pam_keyinit.so force revoke
session include    system-auth
session include    postlogin
-session optional    pam_ck_connector.so
login (END)
```

```
# 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>

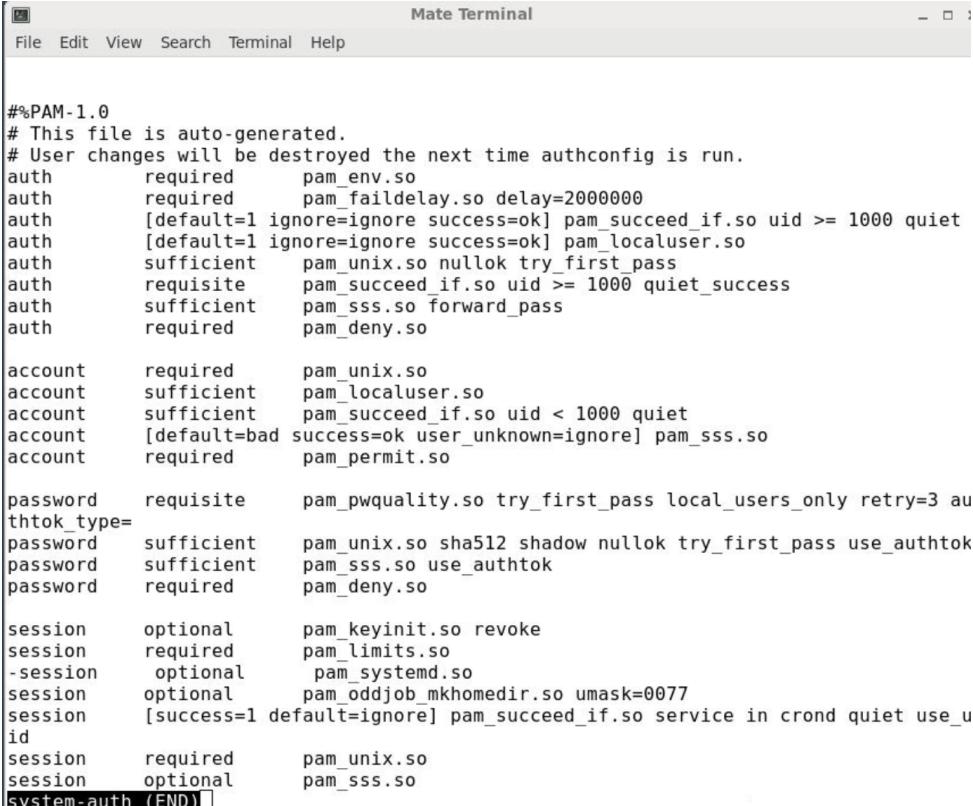
4.3 There are four types of PAM interfaces.

- **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.



```

#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth    required      pam_env.so
auth    required      pam_faildelay.so delay=2000000
auth    [default=1 ignore=ignore success=ok] pam_succeed_if.so uid >= 1000 quiet
auth    [default=1 ignore=ignore success=ok] pam_localuser.so
auth    sufficient   pam_unix.so nullok try_first_pass
auth    requisite    pam_succeed_if.so uid >= 1000 quiet_success
auth    sufficient   pam_sss.so forward_pass
auth    required     pam_deny.so

account required    pam_unix.so
account sufficient  pam_localuser.so
account sufficient  pam_succeed_if.so uid < 1000 quiet
account [default=bad success=ok user_unknown=ignore] pam_sss.so
account required    pam_permit.so

password requisite   pam_pwquality.so try_first_pass local_users_only retry=3 au
thtok_type=
password sufficient  pam_unix.so sha512 shadow nullok try_first_pass use_authtok
password sufficient  pam_sss.so use_authtok
password required    pam_deny.so

session optional    pam_keyinit.so revoke
session required    pam_limits.so
-session optional    pam_systemd.so
session optional    pam_oddjob_mkhomedir.so umask=0077
session [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_u
id
session required    pam_unix.so
session optional    pam_sss.so
system-auth (END)

```

```
# 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.

```
Sep 25 14:17:18 cmhost polkitd[574]: Unregistered Authentication Agent for unix-process:23043:2032947 (system bus name :1.294, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)
Sep 25 14:17:56 cmhost java: pam_securetty(login:auth): cannot determine user's tty
Sep 25 14:17:56 cmhost java: pam_unix(login:auth): check pass; user unknown
Sep 25 14:18:10 cmhost java: pam_securetty(login:auth): cannot determine user's tty
Sep 25 14:18:10 cmhost java: pam_unix(login:auth): check pass; user unknown
Sep 25 14:18:22 cmhost java: pam_securetty(login:auth): cannot determine user's tty
Sep 25 14:18:22 cmhost java: pam_unix(login:auth): check pass; user unknown
Sep 25 14:19:06 cmhost polkitd[574]: Registered Authentication Agent for unix-process:23873:2043715 (system bus name :1.295 [/usr/bin/pktyagent --notify-fd 25 --fallback], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Sep 25 14:19:06 cmhost polkitd[574]: Unregistered Authentication Agent for unix-process:23873:2043715 (system bus name :1.295, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)
Sep 25 14:52:17 cmhost su: pam_unix(su-l:session): session closed for user root
Sep 25 14:52:17 cmhost sudo: pam_unix(sudo:session): session closed for user root
root@cmhost:/var/log#
```

```
# 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.

```
kms:x:39989:39989:Hadoop HDFS:/var/lib/hadoop-kms:/usr/sbin/nologin
atlas:x:39988:39988:Atlas:/var/lib/atlas:/usr/sbin/nologin
schemaregistry:x:39987:39987:Schema Registry:/var/lib/schemaregistry:/usr/sbin/nologin
hue:x:39986:39986:Hue:/usr/lib/hue:/usr/sbin/nologin
zookeeper:x:39985:39985:ZooKeeper:/var/lib/zookeeper:/usr/sbin/nologin
accumulo:x:39984:39984:Accumulo:/var/lib/accumulo:/usr/sbin/nologin
phoenix:x:39983:39983:Phoenix User:/var/lib/phoenix:/usr/sbin/nologin
mapred:x:39982:39982:Hadoop MapReduce:/var/lib/hadoop-mapreduce:/usr/sbin/nologin
druid:x:39981:39981:Druid:/var/lib/druid:/usr/sbin/nologin
ranger:x:39980:39980:Ranger:/var/lib/ranger:/usr/sbin/nologin
zeppelin:x:39979:39979:Zeppelin:/var/lib/zeppelin:/usr/sbin/nologin
oozie:x:39978:39978:Oozie User:/var/lib/oozie:/usr/sbin/nologin
kudu:x:39977:39977:Kudu:/var/lib/kudu:/usr/sbin/nologin
knox:x:39976:39976:Knox:/var/lib/knox:/usr/sbin/nologin
superset:x:39975:39975:Superset:/var/lib/superset:/usr/sbin/nologin
solr:x:39974:39974:Solr:/var/lib/solr:/usr/sbin/nologin
hive:x:39973:39973:Hive:/var/lib/hive:/usr/sbin/nologin
cruisecontrol:x:39972:39972:Cruise Control:/var/lib/cruise_control:/usr/sbin/nologin
impala:x:39971:39971:Impala:/var/lib/impala:/usr/sbin/nologin
rangerraz:x:39970:39970:Ranger Raz User:/var/lib/rangerraz:/usr/sbin/nologin
```

```
# 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 actuality the id_provider is LDAP and the access_provider is Kerberos. Quit the less command.

```
[domain/example.com]
cache_credentials = True
krb5_store_password_if_offline = True
ipa_domain = example.com
id_provider = ipa
auth_provider = ipa
access_provider = ipa
ipa_hostname = cmhost.example.com
chpass_provider = ipa
dyndns_update = True
ipa_server = _srv_, ipa.example.com
dyndns_iface = *
ldap_tls_cacert = /etc/ipa/ca.crt
enumeration = true

[sssd]
services = nss, sudo, pam, ssh

domains = example.com
[nss]
homedir_substring = /home

[pam]

[sudo]

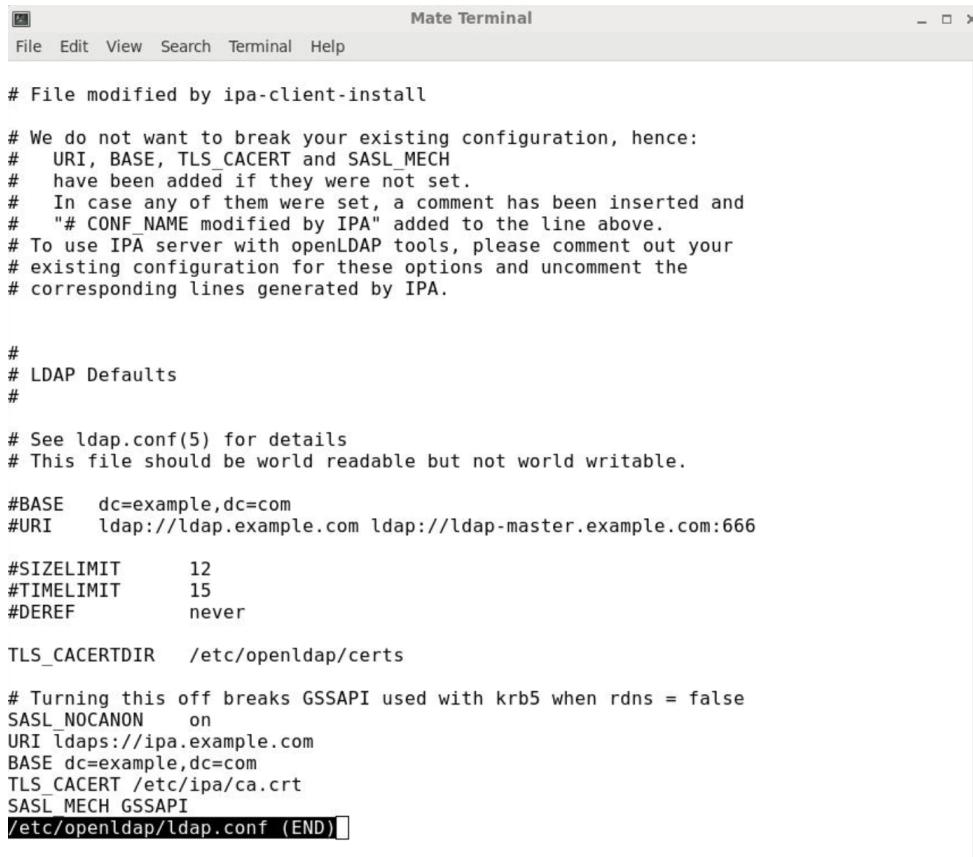
[autofs]

[ssh]
```

```
# 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.



The screenshot shows a terminal window titled "Mate Terminal". The window contains the configuration file /etc/openldap/ldap.conf. The file includes comments about existing configuration, LDAP defaults, and specific connection details like URI, BASE, and TLS settings. It also specifies a TLS certificate directory and SASL mechanisms. The file ends with a closing bracket "]" at the bottom.

```
# File modified by ipa-client-install
#
# We do not want to break your existing configuration, hence:
#   URI, BASE, TLS_CACERT and SASL_MECH
#   have been added if they were not set.
#   In case any of them were set, a comment has been inserted and
#   "# CONF_NAME modified by IPA" added to the line above.
# To use IPA server with openLDAP tools, please comment out your
# existing configuration for these options and uncomment the
# corresponding lines generated by IPA.

#
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

#BASE    dc=example,dc=com
#URI     ldap://ldap.example.com ldap://ldap-master.example.com:666

#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never

TLS_CACERTDIR  /etc/openldap/certs

# Turning this off breaks GSSAPI used with krb5 when rdns = false
#SASL_NOCANON  on
#URI ldaps://ipa.example.com
#BASE dc=example,dc=com
#TLS_CACERT /etc/ipa/ca.crt
#SASL_MECH GSSAPI
/etc/openldap/ldap.conf (END)
```

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

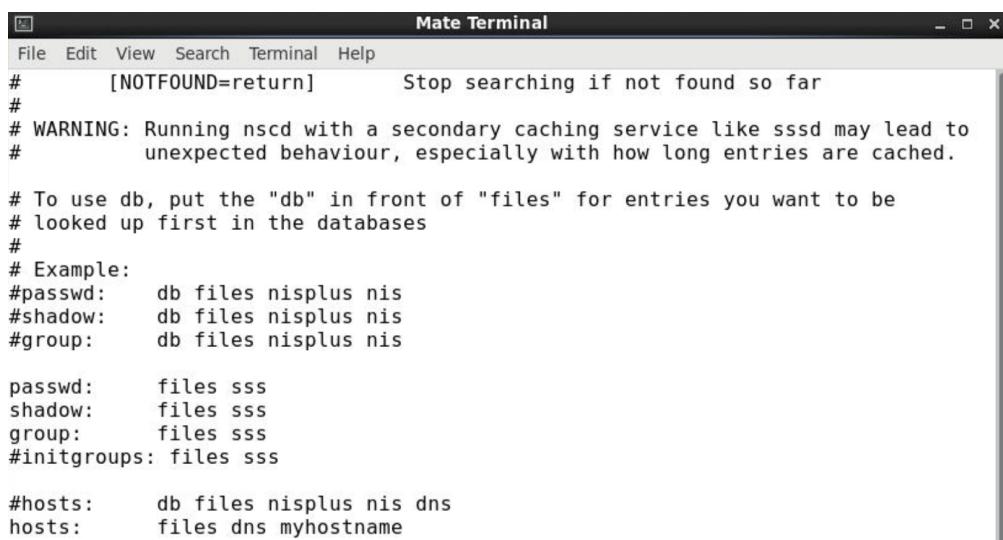
7.2 Use the less command to display the /etc/krb5.conf file. These properties of default_realm, kdc, admin_server, and default_domain define the connection to the Kerberos Key Distribution Center (KDC). Quit the less command.



```
[libdefaults]
default_realm = EXAMPLE.COM
dns_lookup_kdc = false
dns_lookup_realm = false
ticket_lifetime = 86400
renew_lifetime = 604800
forwardable = true
default_tgs_enctypes = aes128-cts-hmac-sha1-96 aes256-cts-hmac-sha1-96
default_tkt_enctypes = aes128-cts-hmac-sha1-96 aes256-cts-hmac-sha1-96
permitted_enctypes = aes128-cts-hmac-sha1-96 aes256-cts-hmac-sha1-96
udp_preference_limit = 1
kdc_timeout = 3000
[realms]
EXAMPLE.COM = {
    kdc = ipa.example.com
    admin_server = ipa.example.com
    default_domain = example.com
}
[domain_realm]
example.com = EXAMPLE.COM
/etc/krb5.conf (END)
```

```
# 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.



```
#      [NOTFOUND=return]          Stop searching if not found so far
#
# WARNING: Running nsqd with a secondary caching service like sssd may lead to
#           unexpected behaviour, especially with how long entries are cached.

# To use db, put the "db" in front of "files" for entries you want to be
# looked up first in the databases
#
# Example:
#passwd:    db files nisplus nis
#shadow:    db files nisplus nis
#group:    db files nisplus nis

passwd:    files sss
shadow:    files sss
group:    files sss
#initgroups: files sss

#hosts:     db files nisplus nis dns
hosts:     files dns myhostname
```

```
# 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.

The screenshot shows the Red Hat Customer Portal interface. At the top, there's a navigation bar with the Red Hat logo, "Red Hat Customer Portal", a search icon, and language options ("English", "All Red Hat"). Below the navigation is a breadcrumb trail: "Products & Services" > "Product Documentation" > "Red Hat Enterprise Linux" > "7" > "System-Level Authentication Guide" > "Chapter 10. Using Pluggable Authentication Modules (PAM)".

The main content area has a sidebar on the left with "System-Level Authentication Guide" and a list of chapters:

- 1. Introduction to System Authentication
 - 1.1. Confirming User Identities
 - 1.2. As Part of Planning Single Sign-On
 - 1.3. Available Services
- I. System Logins
 - 2. Configuring System Authentication

The main content area displays the title "CHAPTER 10. USING PLUGGABLE AUTHENTICATION MODULES (PAM)" and a paragraph about PAMs:

Pluggable authentication modules (PAMs) are a common framework for authentication and authorization. Most system applications in Red Hat Enterprise Linux depend on underlying PAM configuration for authentication and authorization.

A "Feedback" button is located in the top right corner of the main content area.