PAM Prevention

Introduction and/or Background
Linux-PAM (short for Pluggable Authentication Modules which evolved from the Unix-PAM architecture) is a powerful suite of shared libraries used to dynamically authenticate a user to applications (or services) in a Linux system.

Not all applications are 'PAM aware'. You can validate whether a particualar application is PAM capable using the following command:

```
sudo ldd <program location> | grep libpam.so
```

If the libpam.so file is part of the construction of the application then it is capable of managing user access via PAM.

Why use PAM? Well the first is of course security related. But PAM can also save money. If a company has 500 employees but only acquried 25 licenses for a particular program, PAM allows the administrator to whitelist who has access to those licenses by the accounts permitted.

Objectives
In this project/lab the student will:
- Gain familiarity with PAM

Equipment/Supplies Needed
- As specified in Lab 0.0.1.
- Linux Installation File: Ubuntu Server and Ubuntu Desktop

Procedure
Perform the steps in this lab in the order they are presented to you. Answer all questions and record the requested information. Use the Linux Virtual Machine to perform lab activities as directed. Unless otherwise stated, all tasks done as a non-root user. If root access is needed use the sudo command.

Assignment

Activate VMSVR2 and VMPC1 if not already running.

Perform initial configurations on VMSVR2.

Create a new test user account on the VMSVR2 and assign a new account testuser with a password of Password1.

0.i sudo useradd testuser
0.ii passwd testuser

Note the server's IPv4 address.

Verify SSH Server Access

On VMPC1.
Open a terminal window, promote to root, and enter

0.i apt-get install putty

Use the PuTTY SSH Client to ssh into the Ubuntu Server using the test user created above.
Enter the "whoami" command

0.a whoami

take a screenshot.

Exit the session:

0.b exit

Deny testuser Telnet Access

Switch back to the VMSVR2.
Edit PAM's sshd authentication module.

0.c sudo vim /etc/pam.d/sshd

Scroll to the bottom and add the following lines:

```
#Denied user list
auth required pam_listfile.so \
        onerror=succeed item=user sense=deny file=/etc/ssh/deniedusers
```

Create and open a deniedusers file.

0.d sudo vim /etc/ssh/deniedusers

Add a line containing the name of the user to be denied access.

0.e Testuser

Save the file.
Set the required permissions:

```
sudo chmod 600 /etc/ssh/deniedusers
```

Verify denied access

Switch to the VMPC1.
Open the PuTTY SSH Client and attempt to log onto the Ubuntu Server using the test user's account information.
Take a screenshot of the access denied message.

Rubric

Checklist/Single Point Mastery

Concerns Working Towards Proficiency	Criteria Standards for This Competency	Accomplished Evidence of Mastering Competency
	Criteria #1: Screenshot showing whoami command (50 points)	
	Criteria #2: Screenshot showing access denied message (50 points)	