SELinux Security

Introduction and/or Background

Security-Enhanced Linux (SELinux) is a mandatory access control (MAC) security mechanism implemented in the kernel. SELinux was first introduced in CentOS 4 and significantly enhanced in later CentOS releases. These enhancements mean that content varies as to how to approach SELinux over time to solve problems.

Objectives

In this project/lab the student will:

- Gain familiarity with SELinux

Equipment/Supplies Needed

- As specified in Lab 0.0.1.
- Linux Installation File: OVA1 VM, located here.

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

Load and power on the OVA1 VM (Kali currently has issues with SELinux).

The credentials are:

1. Login: user1
2. Pass: tstc

Open a terminal and switch to the root user:

3. su -

You may need to check if selinux is available. Check your repositories and see if selinux-basics is installed. If yes move to step 5. If not then execute --

4 sudo apt-get install selinux-basics selinux-policy-default auditd

View the rules that SELinux uses by default:

5 semanage boolean -l | less

View each entry's column headings:

6 semanage boolean -l | grep 'lp'

View the rule that SELinux uses for pings:

7 semanage boolean -l | grep user_ping

Open a terminal and create a new regular user.

7.a useradd –c "Regular User" regularuser
7.b passwd regularuser
7.c <Pick a password>

Place the regular user in the standard users security group:

8 semanage login -a -s user_u regularuser

Note: The following error (if it appears) can be safely ignored:

```
ValueError: Login mapping for regularuser is already defined
```

View SELinux's user security group list:

9 semanage login -l

Take a screenshot showing the login names and their respective SELinux User status.

Check SELinux's default operating status:

10 sestatus

Take a screenshot of the command's output. It should be operating in permissive mode.

Switch users to the regular user account.

11 ping 127.0.0.1. This should succeed.

Exit back to the root user account.

Change SELinux's mode to enforcement:

12 setenforce 1

Take a screenshot of the command's output. It should be operating in enforcing mode.

Switch users back to the regular account.

13 Ping 127.0.0.1 again. This should not work – wait a few seconds and press Ctrl+C to cancel the command.

Exit back to the root user account.

Change SELinux's mode back to permissive:

14 setenforce 0

Log back into the regular user account and ping 127.0.0.1. They should succeed again.

Exit back to the root user account.

Search the audit log files for ping messages:

15 ausearch –m avc –c ping

Take a screenshot of the ausearch output.

Rubric

Checklist/Single Point Mastery

Concerns Working Towards Proficiency	Criteria Standards for This Competency	Accomplished Evidence of Mastering Competency
	Criteria #1: Screenshot showing the login names and their respective SELinux User status (25 points)	
	Criteria #2: Screenshot showing sestatus output (25 points)	
	Criteria #3: Screenshot showing output of setenforce1 output (25 points)	

	Criteria #4: Screenshot showing ausearch output (25 points)	