

# LAB - 06

- ☐ All screenshots, **must have your username** at command prompt and screenshot should be legible. Snipping tool is advised for the screen shots, no full page screenshot.
- ☐ For **LAB REPORT**, The screenshots should be pasted in Word Document in order of the lab questions and submitted in Blackboard as a single document only. **Plagiarism is awarded zero.**
- ☐ Refer to course details posted in BB for more info on Lab report and screenshots.
- ☐ Do NOT login as root or user with UID=0 to do the lab, use sudo ONLY when required.
- ☐ Do not use changeme username to do the lab, the lab(s) MUST be done using your own username as specified in PART-B of LAB-1
- ☐ Strictly NO screenshots with full screen of terminal or desktop or partly taken screenshots
- ☐ It is highly required to following naming conventions and instructions and it would affect evaluation.

## PRE LAB SHOULD HAVE BEEN COMPLETED FOR THIS LAB

### In-class Activity: 31 - 49

### In toronto VM

### PART-H: SELINUX

31. Check status of SELinux and current mode of SELinux
32. Check the selinux context set on currently logged in user (SCREENSHOT)
33. List selinux context of all process (SCREENSHOT)
34. List selinux context for files in your home directory (SCREENSHOT)
35. List the available selinux users (SCREENSHOT)
36. List selinux context for ports (SCREENSHOT)
37. Using **semanage** list Booleans (SCREENSHOT)
38. Using **semanage** list Booleans and filter for httpd (SCREENSHOT)
39. Using **sestatus** list Booleans and filter for nfs (SCREENSHOT)
40. Using **getsebool** list SELinux Booleans and filter for nfs\_export (SCREENSHOT)
41. Change the status of **nfs\_export\_all\_ro** to off (SCREENSHOT) and then change it back to on (SCREENSHOT)
42. Display report on security contexts set on files and process that are listed in **/etc/sestatus.conf** as per screenshot shown in SCREENSHOT-A (SCREENSHOT)
43. Create a directory **/setest1** and using **chcon** command change selinux user to **staff\_u** and selinux context to **public\_content\_t**. (SCREENSHOT)
44. Create a directory **/setest2** and using **semanage** and **restorecon** change selinux context to **public\_content\_t**. (SCREENSHOT)
45. List the SELinux mapped users. (SCREENSHOT)
46. Create user **seluser1**, and then map to SELinux user **user\_u** and list the mapping (SCREENSHOT)
47. SELinux mapping should be done while creating the user seluser2 and map to SELinux user **staff\_u** and list it. (SCREENSHOT with user creation command and then showing the user selinux mapping)

SCREENSHOT- A	
SELinux status:	enabled
SELinuxfs mount:	/sys/fs/selinux
SELinux root directory:	/etc/selinux
Loaded policy name:	targeted
Current mode:	enforcing
Mode from config file:	enforcing
Policy MLS status:	enabled
Policy deny unknown status:	allowed
Max kernel policy version:	31
Process contexts:	
Current context:	unconfined_u:unconfined_r:unconfined_t:s0-s0:c0,c1023
Init context:	system_u:system_r:init_t:s0
File contexts:	
Controlling terminal:	unconfined_u:object_r:user_devpts_t:s0
/etc/passwd	system_u:object_r:passwd_file_t:s0
/etc/shadow	system_u:object_r:shadow_t:s0
/bin/bash	system_u:object_r:shell_exec_t:s0
/bin/login	system_u:object_r:login_exec_t:s0
/bin/sh	system_u:object_r:bin_t:s0 -> system_u:object_r:shell_exec_t:s0
/sbin/agetty	system_u:object_r:agetty_exec_t:s0
/sbin/init	system_u:object_r:bin_t:s0 -> system_u:object_r:init_exec_t:s0
/usr/sbin/sshd	system_u:object_r:sshd_exec_t:s0

# LAB - 06

- 
48. Display current SELinux mode (**SCREENSHOT**), then change SELinux mode to **permissive** in command line (**SCREENSHOT**), reboot and display the SELinux mode(**SCREENSHOT**) (*Is SELinux mode permissive or enforcing ?*)
49. Try changing permanently to **permissive** and then revert to **enforcing** as permanent.
- 

## **PART-I: SALES (no sudo command must be used)**

50. Login as **sales** department's manager and create directory named **common** in **/sales**
51. Create two files **sales1** and **sales2** with text "**sales**" in **/sales** and set user and group read and write and others no permission for the files **sales1** and **sales2**
52. Provide permission such that this **/sales/common** directory is **r** and **w** for user and group, and others **r** permission
53. Create file **salescommon** with text "**salescommon**" in **/sales/common**,
54. Provide permission such that file **salescommon** is **r** and **w** for user and group, and others **r** permission then **exit** the **sales** user.

**SCREENSHOT:** a) `df -Th /finance /hrd /sales /tech` b) `sudo ls -ld /finance /hrd /sales /tech` c) `sudo ls -lR /finance /hrd /sales /tech`

## **PART-J: PERMISSIONS CHECK (no sudo command be used)**

55. Login as any finance user and test the permission of **/finance, /hrd, /sales, /tech** (**SCREENSHOT**)
56. Login as any hrd user and test the permission of **/finance, /hrd, /sales, /tech**
57. Login as any sales user and test the permission of **/finance, /hrd, /sales, /tech**
58. Login as any tech user and test the permission of **/finance, /hrd, /sales, /tech**
59. Login as John Smith and test the permission of **/finance, /hrd, /sales, /tech**
- =====