# **Exam 1**

## Set Up Work

Run the ‘*sudo –i’* command

**Change directory to /scenariolabs/Exam**

**Run the prep command**

**./prepExam**

**The program will ask for a number, 1-4. Since this is Exam1, respond with 1.**

**The program will now ask you for a password, your instructor will give you the password needed.**

**You should now see a subdirectory ‘Exam1’. Go into this directory and run the programs as instructed.**

# **Exam 1**

## **Question 1**

**Please from run**

**/scenariolabs/Exam/Exam1/Q1**

**to set up the fault.**

**A member of the HR Department, Oscar Pentonville, is unable to login. He can’t remember his password. His login is simply ‘Oscar’. At the very least, you will need to reset his password, and ask him to try logging in. Please do NOT delete his account but rather repair it.**

**You can simulate Oscar logging in by using ssh Oscar@localhost. When he logs in, there should be no errors.**

**Check bad login (see loggins)**

Try see the last bad login: lastb | head

**Try see bad login in messages: tail /var/log/messages**

**Try to look at the rsylog file: cat /etc/rsyslog.conf**

**Try: grep "Failed password" /var/log/messages | head -3**

nano /etc/rsyslog.conf (NB: change the line with authpriv.emerg to authpriv.none)

systemctl restart rsyslog

tail /var/log/messages | grep oscar (NB: shows nothing as it should)

tail /var/log/secure | grep oscar (NB: shows bad loggins)

Check invalid user (loggin narrative)

can try: tail /var/log/audit/audit.log | grep USER (but it will not show which account they were trying to login as)

check if the login attempt was from an invalid user: tail /var/log/secure

might need to change rsyslog.conf: nano /etc/rsyslog.conf

change:

authpriv.\* /var/log/secure

to

authpriv.\* /var/log/secure

authpriv.error /var/log/authpriv.error

systemctl restart rsyslog

tail /var/log/secure (see invalid user)

tail /var/log/authpriv.error

if invalid user then you need to add them: useradd oscar

give Oscar password: passwd oscar

**Check if Locked user (see users and groups)**

**Check if locked: passwd -S oscar (will say locked)**

**Check using grep if locked: grep ‘oscar’ /etc/shadow (look for !!)**

**If locked then you can unlock with: passwd -u oscar**

**Check if Password settings**

**Check to see Oscars password settings: chage -l oscar**

**Check maximum password age, if 0 then increase the number to 99. I think it means 99 days.**

**chage oscar**

**Home directory settings**

**Check in passwd: grep ‘oscar’ /etc/passwd**

**If the home directory is wrong we can change using: usermod -d /home/oscar oscar**

**Check if changed in passwd: grep ‘oscar’ /etc/passwd**

**Run a password check: pwck**

**Reset password**

**Can always reset password: passwd oscar**

## **Question 2**

**Please run**

**/scenariolabs/Exam/Exam1/Q2**

**to set up the fault.**

**A careful eye is being kept on the system memory usage as there have been resource contention issues in the recent past. The file /var/tmp/meminfo\_log is supposed to be updated every five minutes. This is not happening. That’s all you know! Try to get the system working as it should. Make sure it runs.**

## **Question 3**

**Please run**

**/scenariolabs/Exam/Exam1/Q3**

**to set up the fault.**

**Log in as instructor. Change directory into 2 or 3 directories including /tmp. Run the command ls –l in each directory. You will see that you never see the username and group name listed, but instead you may see a number in place of the username or group name, or both. This fault is happening for every user on the system *except root.***

**The system suffered from an administrative mishap. The directories /var and /etc were deleted but have now been restored. That is all you know.**

**Please get the system back to normal as soon as possible.**

**HINT: The inode holds the users’s ID and NOT the users name which is in the output of the ls -l command.**

*(Environment: Azure)*