# **Exam 2**

**Change directory to /scenariolabs/Exam**

**Change directory to /scenariolabs/Exam**

**Run the prep command**

**./prepExam**

**The program will ask for a number, 1-4. Since this is Exam2, respond with 2.**

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

**You should now see a subdirectory ‘Exam2’. Go into this directory and run the programs as instructed.**

# **Exam 2**

## **Question 1**

**Please run**

**/scenariolabs/Exam/Exam2/Q1**

**to set up the fault.**

**A new person has joined the HR department. Oscar Pentonville. He has been given a unix login. His login is simply ‘oscar’ (password=S@nit1zer). Sadly Oscar cannot log in. He has never been able to login. His account was created in a hurry by a member of staff who has now gone away on leave and is not contactable. Try to give Oscar access to the system by repairing his faulty account. Please do NOT delete his account.**

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

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

**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.**

**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**

**Can always reset pass word: passwd Oscar**

## **Question 2**

**Please run**

**/scenariolabs/Exam/Exam2/Q2**

**to set up the fault.**

**Payroll are testing a new application. It has been misconfigured and they cannot connect to it to stop it, which they need to do before they are able to restart it with a corrected configuration. They want you to identify their rogue application and stop it.**

## **Question 3**

**Please run**

**/scenariolabs/Exam/Exam2/Q3**

**to set up the fault.**

**Log in to the Linux system as instructor. Type the command ‘ls –l’. You will see numbers where group names should be. Try doing this on /tmp too. You will see the same problem no matter where you look and it’s the same for all other users except for 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 maybe.**

**HINT: The inode contains the group ID and not the group name, which is output by the ‘ls -l’ command.**

*(Environment: Azure)*