Scenario

Lucky_Duck_Investigations/Roulette_loss_Investigation

You have just been hired by Lucky Duck Casino as a security analyst.

- Lucky Duck has experienced a significant loss of money on the roulette tables over the last month.
- More specifically, the largest losses occurred on March 10th, 12th, and 15th.
- Your manager believes there is a player working with a Lucky Duck dealer to cheat at roulette.
- The casino contains a vast database containing data on wins and losses, player analysis and dealer schedules.

You are tasked with navigating, modifying, and analyzing these data files in order to provide evidence that can implicate the fraudulent player and dealer.

- You will prepare several evidence files to assist with prosecution of the casino player and the rogue dealer.
- You must work quickly as Lucky Duck can't afford any more losses!

Lab Environment

- You will use your local Vagrant virtual machine for today's activities. Please note that instructors and students have different access credentials.
    - Username:sysadmin
    - Password: cybersecurity

Files Required

Lucky Duck Casino has provided you with the following files if required:

- **Note**: Your instructions will have you set up the files via a wget command, but they are also provided in compressed zip format if the command does not work.
    - Win/loss player data from the roulette tables during the week of March 10th

    - Employee Dealer schedule during the week of March 10th

Your Objective

Utilize your command line skills to determine who is the Casino Cheat and Rogue Roulette Dealer colluding to scam Lucky Duck out of thousands of dollars!

After your investigation you will provide the following:

- A summary of your findings for each step.
- A conclusion of your findings to provide to the authorities.

Topics Covered in This Assignment

- Making directories
- Previewing files
- Making and editing files with touch and nano
- Counting data with wc
- Navigating Through Directories
- Using grep to search through files
- Using awk to isolate out data
- Redirecting and appending data into files
- Designing a Shell Script
- Using Arguments in a Shell Script

Let's get started!

Lucky Duck Security Investigation Instructions

Step 1: Investigation Preparation

Your first task is to set up directories to prepare for your investigation.

- Begin by making a single directory titled Lucky_Duck_Investigations.

- Next, within this directory of Lucky_Duck_Investigation, create a directory for this specific investigation titled Roulette_loss_Investigation.

- Within Roulette_loss_Investigation, create the following directories:

    - Player_Analysis to investigate the Casino Player.
    - Dealer_Analysis to investigate the Dealers.
    - Player_Dealer_Correlation to summarize your findings of the collusion.

- Create empty files called Notes_<Directory Name> under each of those subdirectories to be used later to add in any investigation notes.
    - For example: Notes_Player_Analysis

Step 2: Gathering Evidence

Your next task is to move evidence from the specific days Lucky Duck experienced heavy losses at the roulette tables.

- Navigate to the directory where you created the Lucky_Duck_Investigations directory and run the following command to setup the evidence files:

  wget "https://tinyurl.com/3-HW-setup-evidence" && chmod +x ./3-HW-setup-evidence && ./3-HW-setup-evidence

- After running this command your current directory should have the following subdirectories:
    - Dealer_Schedules_0310: contains the dealer schedules
    - Lucky_Duck_Investigations: contains the investigation directories and notes files you created
    - Roulette_Player_WinLoss_0310: contains the data for player wins and losses
- The Dealer_Schedules_0310 and Roulette_Player_WinLoss_0310 directories contain the win/loss player data from the roulette tables during the week of March 10th.
    - Since the losses occurred on March 10th, 12th, and 15th, move those files into the directory Player_Analysis.

mv Lucky_Duck_Investigations/Roulette_Player_WinLoss_0310/0310_win_loss_player_data Lucky_Duck_Investigations/Roulette_loss_Investigation/Player_Analysis

    - Since the losses occurred on March 10th, 12th, and 15th, move the schedules for those days into the directory Dealer_Analysis

/home/sysadmin/Lucky_Duck_Investigations/Roulette_loss_Investigation/Dealer_Analysis

mv Lucky_Duck_Investigations/Dealer_Schedules_0310/0315_Dealer_schedule Lucky_Duck_Investigations/Roulette_loss_Investigation/Dealer_Analysis

Step 3: Correlating the Evidence

Your next task is to correlate the large losses from the roulette tables to the dealer schedule in order to determine the dealer and player that are likely colluding to steal money from Lucky Duck.

- *Note: Any winnings for Luck Duck Casino are indicated with a positive number and any losses are a negative number.*

Complete the following tasks:

Player Analysis

- Navigate to the Player_Analysis directory.

- Use grep to isolate all of the losses that occurred on March 10th, 12th, and 15th.

grep - 0310_win_loss_player_data >> Roulette_Losses

grep - 0312_win_loss_player_data >> Roulette_Losses

grep - 0315_win_loss_player_data >> Roulette_Losses

- Place those results into a file called Roulette_Losses.

- Preview your file Roulette_Losses and analyze the data.

- Then, record in the Notes_Player_Analysis file:
  grep -o Mylie Roulette_Losses | wc -w
-
-
    - The times the losses occurred on each day.
    - If there is a certain player that was playing during each of those times.
    - The total count of times this player was playing.
        - Hint: Use the wc command for this value.

Dealer Analysis

- Navigate to the Dealer_Analysis directory.

- This file contains the dealer schedules for the various Lucky Duck casino games: Blackjack, Roulette, and Texas Hold 'Em.

- Preview the schedule to view the format and to understand how the data is separated.

- Using your findings from the player analysis, create a **separate script to look at each day and each time** that you determined where losses occurred. Use awk, pipes, and grep tp isolate out the following four fields:

    - Time
    - AM/PM
    - First name of roulette dealer
    - Last name of roulette dealer
- For example, if there was a loss that occurred on March 10th at 2 PM, you would write one script that found the roulette dealer that was working at that specific day and time.

    - **Hint**: you will have many scripts, but only a small change is required for each script.
- Run all of the scripts and append those results into a file called Dealers_working_during_losses.

grep 05:00:00 0310_Dealer_schedule | head -n 1

cat -n 5 ~/Lucky_Duck_Investigations/Roulette_loss_Investigation/Player_Analysis/Roulette_Losses

- Preview your file Dealers_working_during_losses and analyze the data.

- Record in the Notes_Dealer_Analysis file:

    - The primary dealer working at the times where losses occurred.

    - How many times the dealer worked when major losses occurred.

Player/Employee Correlation

- In notes file of the Player_Dealer_Correlation directory, add your summary of the player and dealer you believe are colluding to scam Lucky Duck.

- Make sure to document your specific reasons for this finding.

Step 4: Scripting your Tasks

You manager is impressed with the work you have done so far on the investigation.

- Your manager has tasked you with building a shell script that can easily analyze future employee schedules. Therefore, we can determine who was the employee working at a specific time in case losses occur again.

- This shell script can be provided to the security department to easily do the same analysis.

Complete the following tasks:

- Remain in the Dealer_Analysis directory.

- Develop a shell script called roulette_dealer_finder_by_time.sh that can analyze the employee schedule to easily find the roulette dealer at a specific time.

    - **Hint**: You will be using a script similar to the one you created for the "Dealer Analysis" step, except do not output the results into a file.
- Design the shell script to accept the following two arguments:

    - One for the date (four digits)
    - One for the time
- **Note**: The argument should be able to accept AM or PM.

- Test your script on the schedules to confirm it outputs the correct dealer at the time specified.

Bonus: In case there is future fraud on the other Lucky Duck Games, create a shell script called roulette_dealer_finder_by_time_and_game.sh that has the three following arguments:

- One for the the specific time

- One for the specific date

- One for the casino game being played

    Hint: The argument does not need to name the specific casino game.

Your Submission

Guidelines for your Submission:

Move the following to the Player_Dealer_Correlation directory:

- All of your note files
- Your Evidence Files:
    - Roulette_Losses
    - Dealers_working_during_losses
- Your Shell script(s)

Submit your findings!

Homework Complete, Great Job!