Task 3 - Shell Scripting

Objective

The objective of this task is to introduce you to Shell Scripting. You will write a simple shell script to display a list of all commands that were run as `sudo` on a Linux system. The goal is to demonstrate the power of scripts for automating common security and administration tasks.

Background

A shell script, in simple terms, is a sequence of shell commands for performing tasks on Unix-based systems. They are perfect for automation and can perform a variety of functions ranging from security, OS administration, auditing, as well as data analysis. While high-level programming languages like C and Python can also be used for automation, shell scripts can execute on almost all modern UNIX, Linux, BSD and Mac OS X operating systems without requiring any additional tools. They are also very easy to implement.

For this simple task, an overview of the Shell Scripting class will suffice. Additionally, knowledge of commands that can read file contents and commands that can search patterns within contents will be useful.

Setup

No setup is required for this task. Ensure that you test your script on the Linux VM before submission.

Requirements

Write a shell script that displays the list of all commands that were run as `sudo` on a Linux system. This script **MUST** be called `parse_sudo`. The script must parse each line of the `/var/log/auth.log` file and print those lines that show a command being run as `sudo`. *Note that this is a very simple task that can be completed in as little as 3 lines of code.*

An example run of the script is shown below. Note that the output on your VM will differ based on your usage of `sudo`. If you don't see any output, ensure that you run a few commands as `sudo` and try again.

```
$ ./parse_sudo

The following commands were run as sudo on this system -
Oct 18 13:56:19 snhp sudo:  sashank : TTY=pts/1 ; PWD=/home/sashank ; USER=root ; COMMAND=
/usr/bin/apt update
Oct 18 13:56:34 snhp sudo:  sashank : TTY=pts/1 ; PWD=/home/sashank ; USER=root ; COMMAND=
/usr/bin/apt upgrade
Oct 18 13:56:46 snhp sudo:  sashank : TTY=pts/1 ; PWD=/home/sashank ; USER=root ; COMMAND=
/usr/bin/apt dist-upgrade
Oct 18 13:56:57 snhp sudo:  sashank : TTY=pts/1 ; PWD=/home/sashank ; USER=root ; COMMAND=
/usr/bin/apt autoremove
Oct 18 13:57:49 snhp sudo:  sashank : TTY=pts/1 ; PWD=/home/sashank ; USER=root ; COMMAND=
/usr/bin/apt install openssh-server
```

Task Report

For this task, each student must submit the `parse_sudo` shell script on Blackboard.

Grading

100 points - Running the script correctly displays a list of all commands that were run as `sudo`