Module 5 Challenge: Archiving and Logging Data

This Challenge assignment is designed to solidify and demonstrate your knowledge of the following concepts and tools:

- Creating a `tar` archive that excludes a directory using the `--exclude=` command option.
- Managing backups using cron jobs.
- Writing bash scripts to create system resource usage reports.
- Performing log filtering using `journalctl`.
- Managing log file sizes using `logrotate`.
- Creating an auditing system to check for policy and file violations using `auditd`.

Feel free to refer to the student guides and slides from this module's lessons as you work through the assignment. If you get stuck, remember that you can also use Google and man pages for more information.

Scenario

For this assignment, you will play the role of a security analyst at Credico Inc., a financial institution that offers checking, savings, and investment banking services.

- The company collects, processes, and maintains a large database of private financial information for both consumer and business accounts.
- The data is maintained on a local server.
- The company must comply with the Federal Trade Commission's Gramm-Leach-Bliley Act (GLBA Links to an external site.), which requires that financial institutions explain their information-sharing practices to their customers and protect sensitive data.

In an effort to mitigate network attacks and meet federal compliance, Credico Inc. developed an efficient log management program that performs:

- Log size management using `logrotate`.
- Log auditing with `auditd` to track events, record the events, detect abuse or unauthorized activity, and create custom reports.

These tools, in addition to archives, backups, scripting, and task automation, contribute to a fully comprehensive log management system.

You will expand and enhance this log management system by learning new tools, adding advanced features, and researching additional concepts.

Challenge Activity: : Lab Environment :

1. create a directory Projects under /home/sysadmin/

    a. -cd /home/sysadmin

    b. -sudo mkdir Projects

    c. Download the TarDocs.tar from online in VM and move it from Downloads to Projects - sudo mv ~/Downloads/TarDocs.tar ~/Projects/

    d. Extract the TarDocs.tar file using - tar xvvf TarDocs.tar. This will create a TarDocs directory with 5 subdirectory within it.

    e. To verify that there is a Java folder - ls -l ~/Projects/TarDocs/Documents/

    f. Now create a tar archive without the Java folder and name it Javaless_Docs.tar - sudo tar cvvWf Javaless_Docs.tar --exclude="TarDocs/Documents/Java" TarDocs/

    g. Verify that Java folder is not in the newly archived TAR File -tar -tvf Javaless_Docs.tar | grep Java this command returns O outputs, hence confirms that the newly created tar file excluded the Java Folder.

Flag question: Question 1

Question 1 **15 pts**

What is the command used to extract the 'TarDocs.tar' archive to the current directory while showing the files being extracted?

tar xvvf TarDocs.tar

Flag question: Question 2

Question 2 **15 pts**

What is the command to create the 'Javaless_Docs.tar' archive from the 'TarDocs/' directory, while excluding the 'TarDocs/Documents/Java' directory?

tar cvvWf Javaless_Docs.tar --exclude="TarDocs/Documents/Java" TarDocs/

What is the command to create the 'Javaless_Docs.tar' archive from the 'TarDocs/' directory, while excluding the 'TarDocs/Documents/Java' directory?

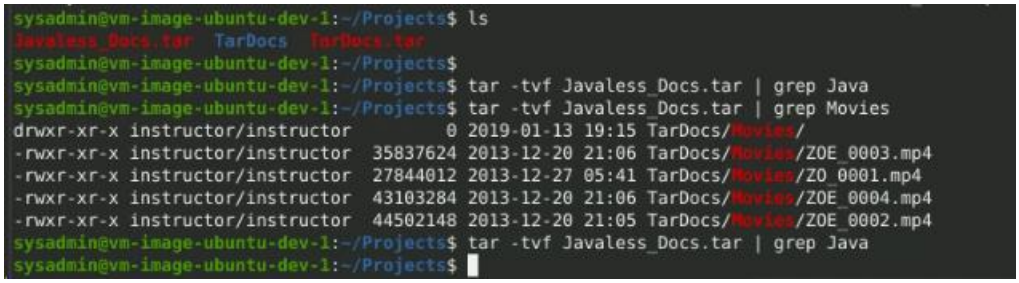
- (●) tar cvvf Javaless_Docs.tar --exclude="TarDocs/Documents/Java" TarDocs/
- ( ) tar Javaless_Docs.tar --exclude="TarDocs/"
- ( ) tar cvvf +include Javaless_Docs.tar -exclude=TarDocs/
- ( ) tar cvf Javaless_Docs.tar -detar="TarDocs/Documents/Java" TarDocs/

Flag question: Question 3

Question 3 **15 pts**

How can you verify that the 'Java/' directory is not in the newly created 'Javaless_Docs.tar' archive?

tar -tvf Javaless_Docs.tar | grep Java



How can you verify that the 'Java/' directory is not in the newly created 'Javaless_Docs.tar' archive?

- (●) tar -tvf Javaless_Docs.tar | grep Java
- ( ) tar Javaless_Docs.tar | find Java
- ( ) tar -tvf find Java | Javaless_Docs.tar
- ( ) tar -f Java ? Javaless_Docs.tar

Flag question: Question 4

Question 4 **15 pts**

What is the cron job command to schedule a weekly backup of the '/var/log/auth.log' file every Thursday at 6:00 AM?

0 6 * * * 4 tar -zcf /auth_backup.tgz /var/log/auth.log

What is the cron job command to schedule a weekly backup of the '/var/log/auth.log' file every Thursday at 6:00 AM?

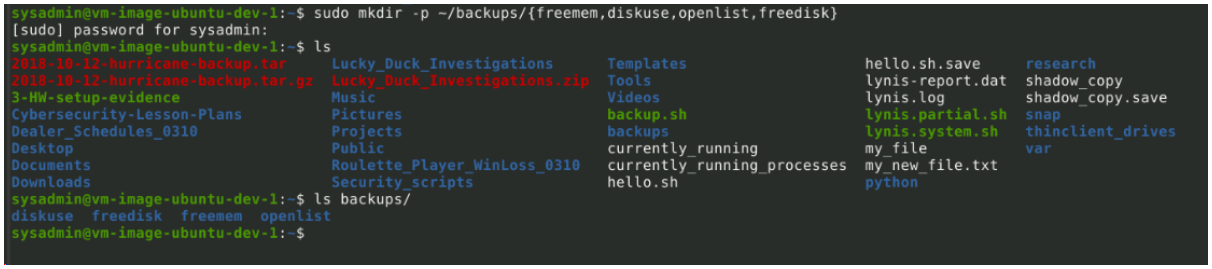
- ○ 0 6 0 0 0 4 tar -zcf /auth_backup.tgz /var/log/auth.log
- ○ 0 0 6 0 0 4 tar -f /auth_backup.tgz /auth.log
- ○ 6 * * * 4 tar -zcf /auth_backup.tgz /var/auth.log
- ◉ 0 6 * * * 4 tar -zcf /auth_backup.tgz /var/log/auth.log

Flag question: Question 5

Question 5 **15 pts**

What is the brace expansion command used to create four subdirectories named 'freemem', 'diskuse', 'openlist', and 'freedisk' within the '~/backups' directory?

sudo mkdir -p ~/backups/{freemem,diskuse,openlist,freedisk}



What is the brace expansion command used to create four subdirectories named 'freemem', 'diskuse', 'openlist', and 'freedisk' within the '~/backups' directory?

- ○ sudo mkdir -insert ~/backups/{freemem,diskuse,openlist,freedisk}
- ◉ sudo mkdir -p ~/backups/{freemem,diskuse,openlist,freedisk}
- ○ sudo mkdir -p ~/backups/(freemem diskuse openlist freedisk)
- ○ sudo mkdr -p ~/{freemem,diskuse,openlist,freedisk}

Flag question: Question 6

Question 6 **15 pts**

How do you make the 'system.sh' script executable?

Chmod +x system.sh

Sudo ./system.sh

How do you make the 'system.sh' script executable?

sudo ./system.sh

Flag question: Question 7

Question 7 **10 pts**

What is the command to copy the 'system.sh' script to the system-wide weekly cron directory?

sudo cp system.sh /etc/cron.weekly

What is the command to copy the 'system.sh' script to the system-wide weekly cron directory?

- (●) sudo cp system.sh /etc/cron.weekly
- ( ) sudo cp /etc/cron.weekly system.sh
- ( ) sudo cp system.sh /etc/weekly.cron
- ( ) sudo cp system.sh /etc/cron.week