CYSE 270: Linux System for Cybersecurity

Assignment-9

Task A - Backup your system (Using crontab) [100 points]

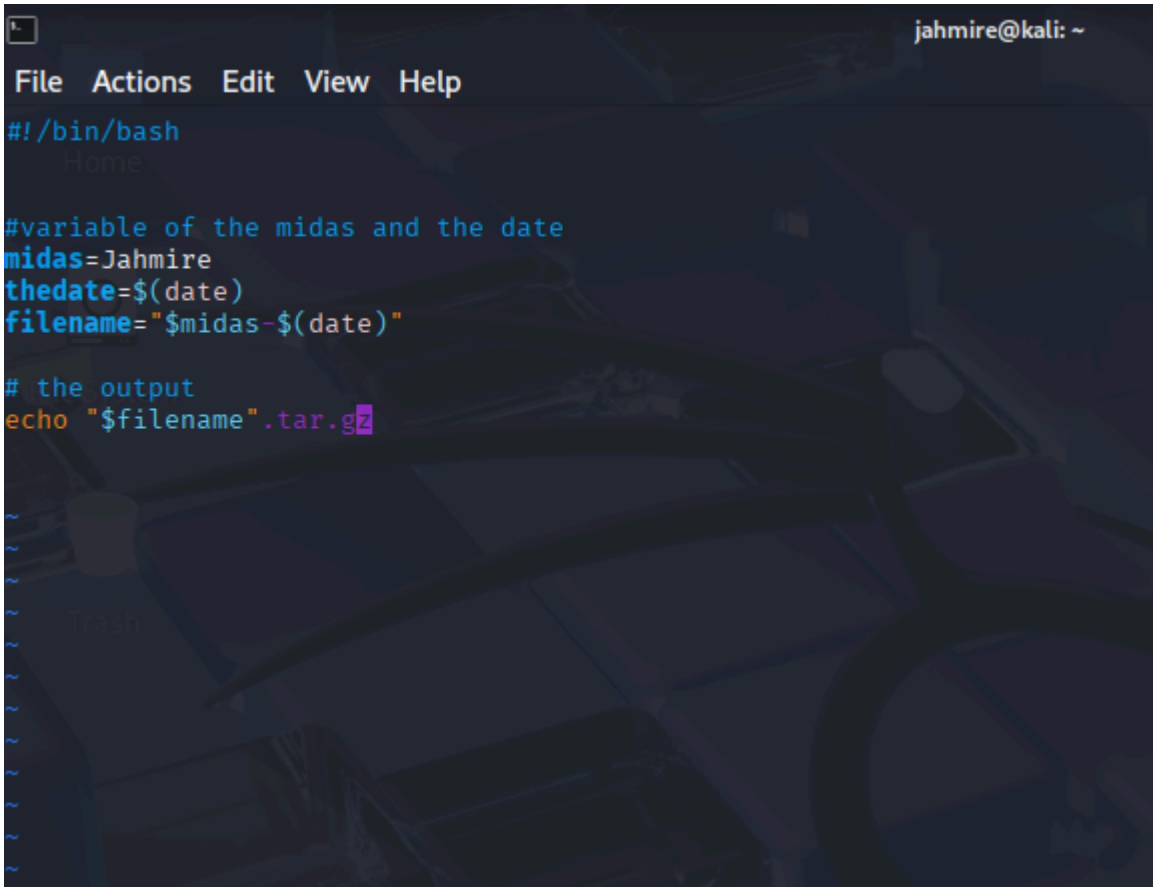
Scenario: Performing system backup can be time-consuming, and the process is often overlooked. For this scenario:

1. **(10 Points)** Create a new user **Alice (with home directory**).

2. **(50 Points) Write a shell script that backups Alice's home directory by creating a tar file (tape archive), using the following steps:**

   a. Do the following:

   - Take **2 inputs** with their values-vi your **MIDAS** name and **current date (for example, midas=Mohammed)**.
   - Create a variable named as **filename** that should be assigned the value as **MIDAS-date** (example output after executing the script would be like, **Mohammed-2024.11.04-22.08.01.tar.gz**).



• Using **tar** command, create a tape archive for Alice's home directory (/home/Alice) and the **filename** created above (in step-2-ii). (Please

learn about tar command in Linux for its usage)

```
re㉿kali)-[~]
tar -cvf Lab9.tar /home/Alice
ssword for jahmire:
ving leading `/' from member names
ce/
ce/.zshrc
ce/.face
ce/.bashrc.original
ce/.zprofile
ce/.profile
ce/.bash_logout
ce/.config/
ce/.config/powershell/
ce/.config/powershell/Microsoft.PowerShell_profile.ps1
ce/.config/cherrytree/
ce/.config/cherrytree/config.cfg
ce/.config/xfce4/
ce/.config/xfce4/panel/
ce/.config/xfce4/panel/genmon-15.rc
ce/.config/nautilus/
ce/.config/nautilus/scripts-accels
ce/.local/
ce/.local/bin/
ce/.local/share/
ce/.local/share/nautilus/
ce/.local/share/nautilus/scripts/
ce/.local/share/nautilus/scripts/Terminal
ce/.face.icon
ce/.java/
ce/.java/.userPrefs/
ce/.java/.userPrefs/burp/
ce/.java/.userPrefs/burp/prefs.xml
ce/.bashrc
```

b. Move the tape archive file/tar file (created in step 2-iii) to /var/backups/ directory using correct command in linux.

```
┌──(jahmire㉿kali)-[~]
└─$ sudo mv Lab9.tar /var/backups/
```

c. To optimize the disk usage, pick a compression algorithm (bz2, gzip, or xv) to compress the tar file you created in /var/backups/ in the previous step-2b. 3. **(30 Points) Create a crontab file to keep the scheduled task running for 3 minutes**, then check the contents in the /var/backups directory. Your output should be look similar to the following:

```
┌──(cyse270㉿CYSE270)-[/home/Alice]
└─$ ls /var/backups
Mohammed-2024.11.04-22.08.01.tar.gz
```

```
┌──(jahmire㉿kali)-[/var/backups]
└─$ sudo gzip Lab9.tar
```

Kali Linux [Running] - Oracle VirtualBox

File Machine View Input Devices Help

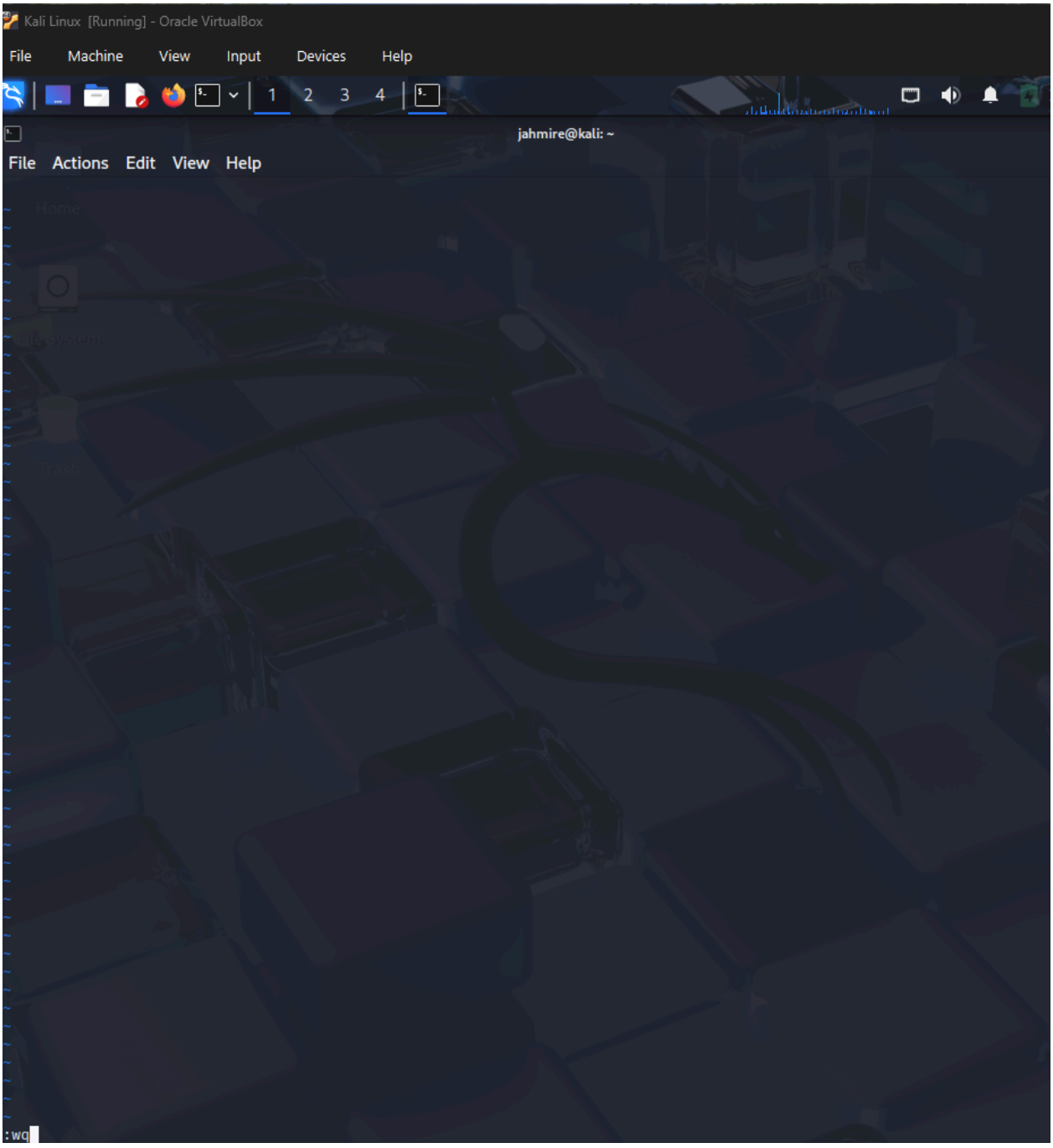
1 2 3 4

jahmire@kali: ~

File Actions Edit View Help

```
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   comman
3 * * * *  ./Lab9,sh
```

4. **(10 Points)** Cancel the crontab jobs.



TASK B: SYSTEM CLEANUP (EXTRA CREDIT) [20 Points]

Scenario: In the above scenario, your system disk will be filled up eventually without cleaning up the old backups. Therefore, in this optional task, create a script that checks

the number of backups you created in Task A. If the number of the backup file is more than a pre-defined threshold, the script will delete the old archives to maintain the backups under a reasonable size.

This script should do the following:

1. Count the number of backups created in Task A and determine if this number is larger than 3.

2. Nothing should happen if the number of backups is less than the threshold, 3.

3. If more backup archives are detected, calculate the number of backups to delete. Then delete the old archives.

Note: As the script needs to write contents in the "/var/backups" folder, which is owned by root, you should consider the permission issue properly. (Using **sudo** to create crontab file)

Reference: How to Format Date for Display or Use In a Shell Script:
https://www.cyberciti.biz/faq/linux-unix-formatting-dates-for-display/

Reference: How to append date timestamp to filename:

https://crunchify.com/shell-script-append-timestamp-to-file-name/