# Project: Brute force Attack

**Problem Statement**

Conduct a comprehensive security assessment and response for a CentOS VM under brute force attack, focusing on log analysis, user verification, and implementation of enhanced security measures to mitigate future threats.

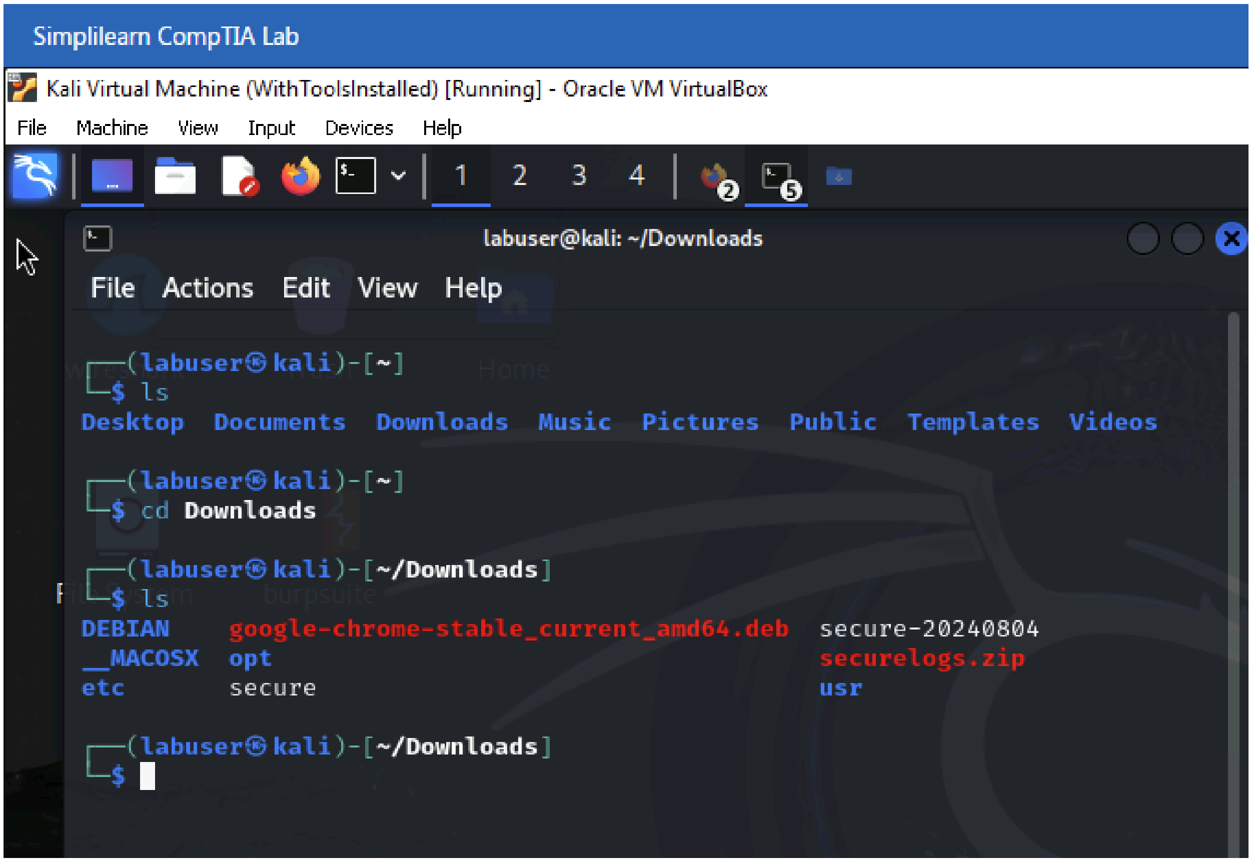
**Tasks:**

1. Download Authentication Logs: Access and download authentication logs from the provided URL. These logs contain critical evidence of brute force attacks, including access attempts and usernames.
2. Analyze the Logs for Usernames: Use log analysis tools or scripts to extract all usernames attempted during the attack, identifying the extent and specific entry points targeted.
3. Cross-Reference Usernames with Company Records: Cross-reference extracted usernames with the internal user database to check if any correspond to actual user accounts, indicating potential insider threats.
4. Implement Security Enhancements: Based on findings, enhance security by enforcing stricter password policies, implementing multifactor authentication, and possibly changing SSH ports.
5. Continuous Monitoring and Reporting: Set up continuous monitoring to detect unusual access patterns and generate regular reports to inform the security team of any new threats.

## Task 1: Download authentication logs

Step 1: I accessed kali linux from simplilearn lab and downloaded the file securelogs.zip and extracted the zip file to downloads folder.

Step 2: Opened Terminal and navigated Downloads directory.



Simplilearn CompTIA Lab
Kali Virtual Machine (WithToolsInstalled) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
labuser@kali: ~/Downloads
File Actions Edit View Help

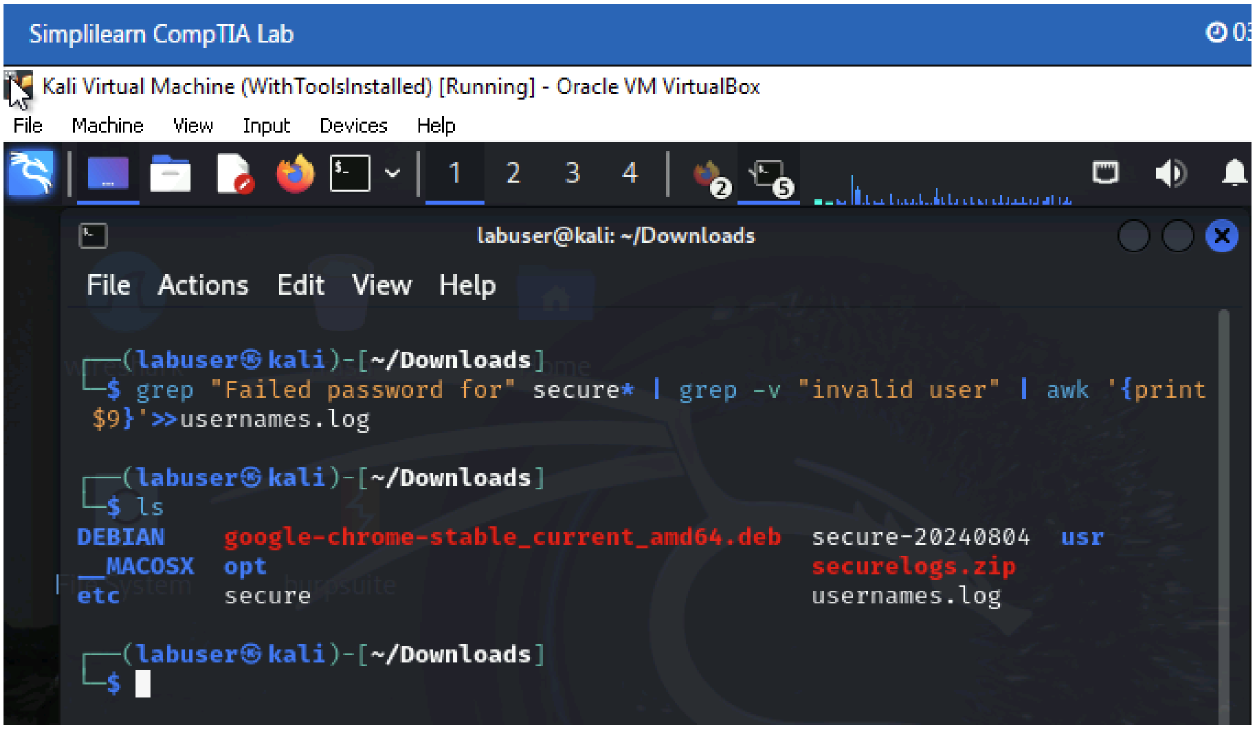
```
┌──(labuser㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(labuser㉿kali)-[~]
└─$ cd Downloads

┌──(labuser㉿kali)-[~/Downloads]
└─$ ls
DEBIAN    google-chrome-stable_current_amd64.deb  secure-20240804
__MACOSX  opt                                     securelogs.zip
etc       secure                                  usr

┌──(labuser㉿kali)-[~/Downloads]
└─$ 
```

## Task 2: Analyze the Logs for Usernames

Step1: Run the following command to extract usernames from SSH failed login attempts and save them to usernames.log

**grep "Failed password for" secure* | grep -v "invalid user" | awk '{print $9}' >> usernames.log**

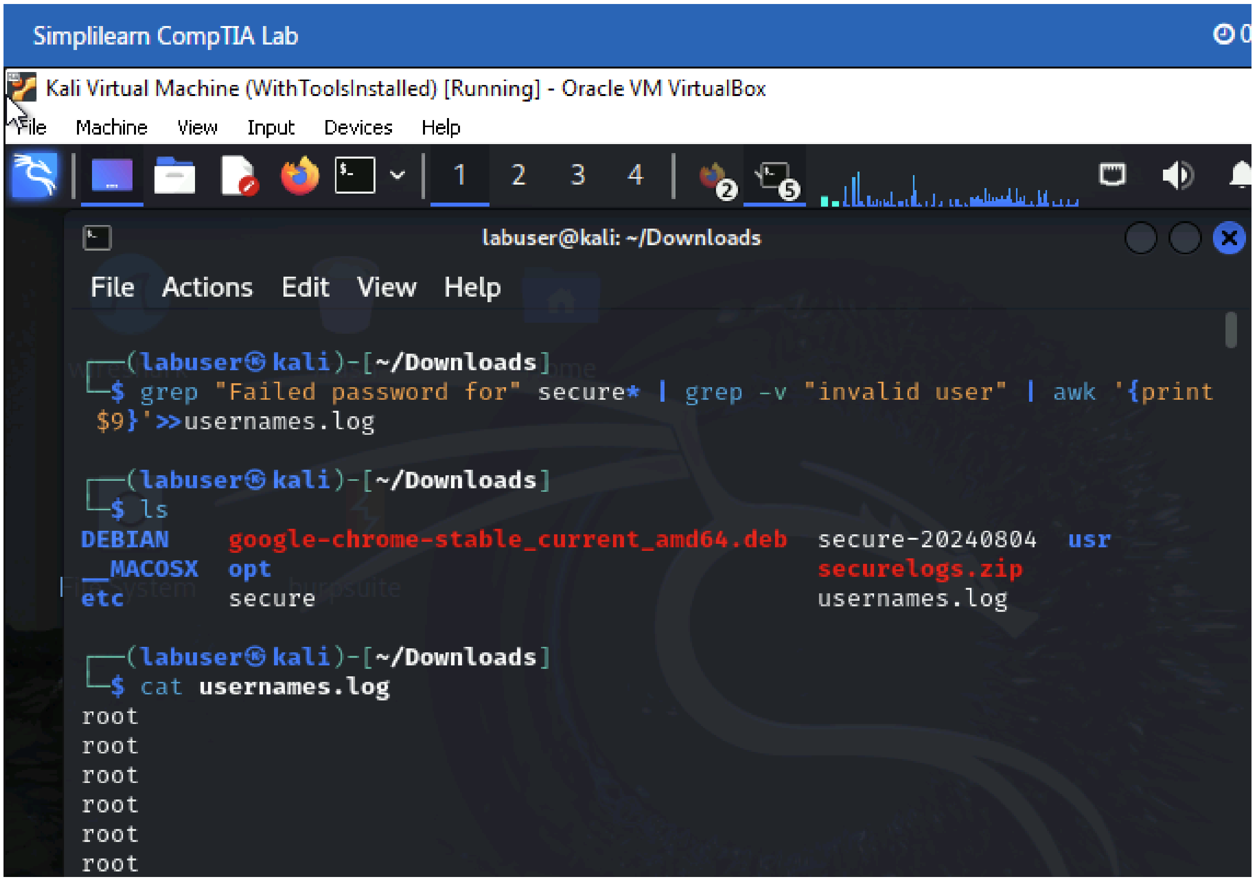
and listed the folder to see whether the file usernames.log file is generated.


Simplilearn CompTIA Lab
Kali Virtual Machine (WithToolsInstalled) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
labuser@kali: ~/Downloads
File Actions Edit View Help

```
┌──(labuser㉿kali)-[~/Downloads]
└─$ grep "Failed password for" secure* | grep -v "invalid user" | awk '{print
$9}'>>usernames.log

┌──(labuser㉿kali)-[~/Downloads]
└─$ ls
DEBIAN    google-chrome-stable_current_amd64.deb  secure-20240804  usr
__MACOSX  opt                                     securelogs.zip
etc       secure                                  usernames.log

┌──(labuser㉿kali)-[~/Downloads]
└─$ 
```

Step 2: To display the extracted usernames and verify the results, run the following command.

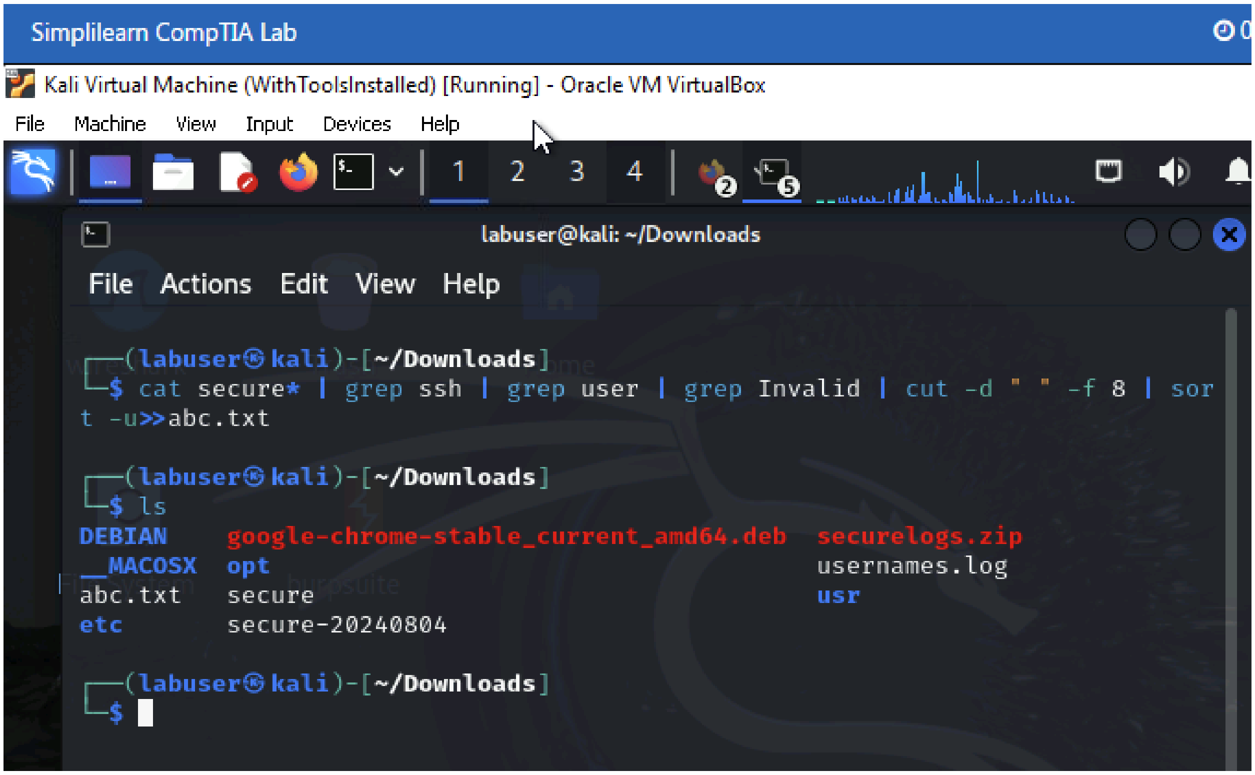
**cat usernames.log**


Simplilearn CompTIA Lab
Kali Virtual Machine (WithToolsInstalled) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
labuser@kali: ~/Downloads
File Actions Edit View Help

```
┌──(labuser㉿kali)-[~/Downloads]
└─$ grep "Failed password for" secure* | grep -v "invalid user" | awk '{print
$9}'>>usernames.log

┌──(labuser㉿kali)-[~/Downloads]
└─$ ls
DEBIAN    google-chrome-stable_current_amd64.deb  secure-20240804  usr
__MACOSX  opt                                     securelogs.zip
etc       secure                                  usernames.log

┌──(labuser㉿kali)-[~/Downloads]
└─$ cat usernames.log
root
root
root
root
root
root
```

Step 3: Run the following command to sort and filter invalid usernames from the logs and save them to abc.txt

**cat secure* | grep ssh | grep user | grep Invalid | cut -d " " -f 8 | sort -u >> abc.txt**

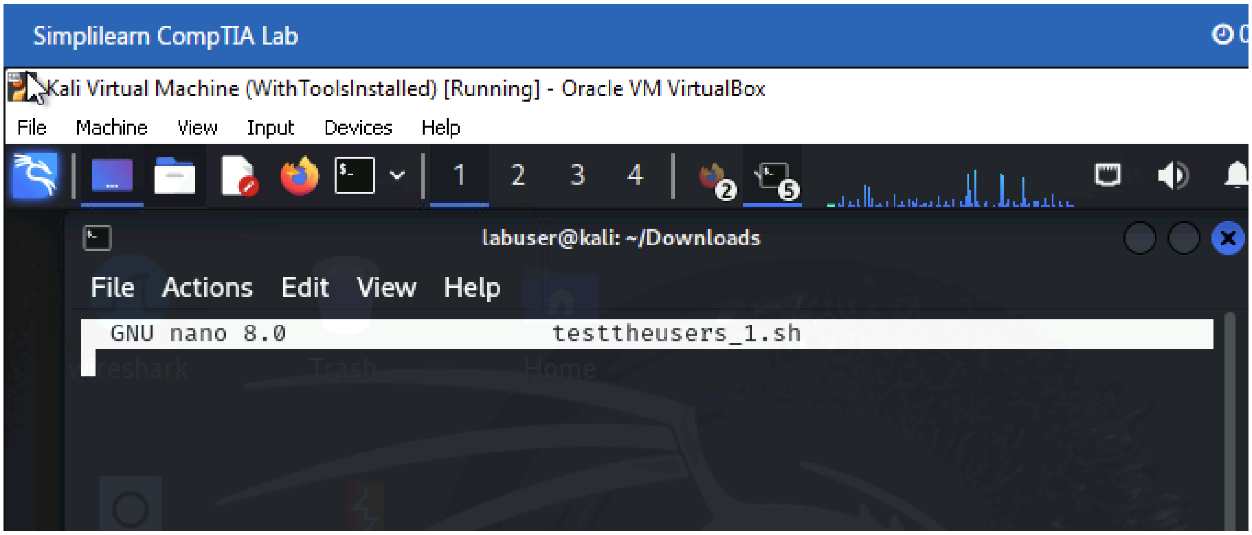

Simplilearn CompTIA Lab
Kali Virtual Machine (WithToolsInstalled) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
labuser@kali: ~/Downloads
File Actions Edit View Help

```
┌──(labuser㉿kali)-[~/Downloads]
└─$ cat secure* | grep ssh | grep user | grep Invalid | cut -d " " -f 8 | sor
t -u>>abc.txt

┌──(labuser㉿kali)-[~/Downloads]
└─$ ls
DEBIAN     google-chrome-stable_current_amd64.deb  securelogs.zip
__MACOSX   opt                                     usernames.log
abc.txt    secure                                  usr
etc        secure-20240804

┌──(labuser㉿kali)-[~/Downloads]
└─$ 
```

## Task 3: Cross-Reference Usernames with Company Records:

Step 1: Run the following command to create a script named testtheusers_1.sh to check if extracted usernames exist in the /etc/passwd

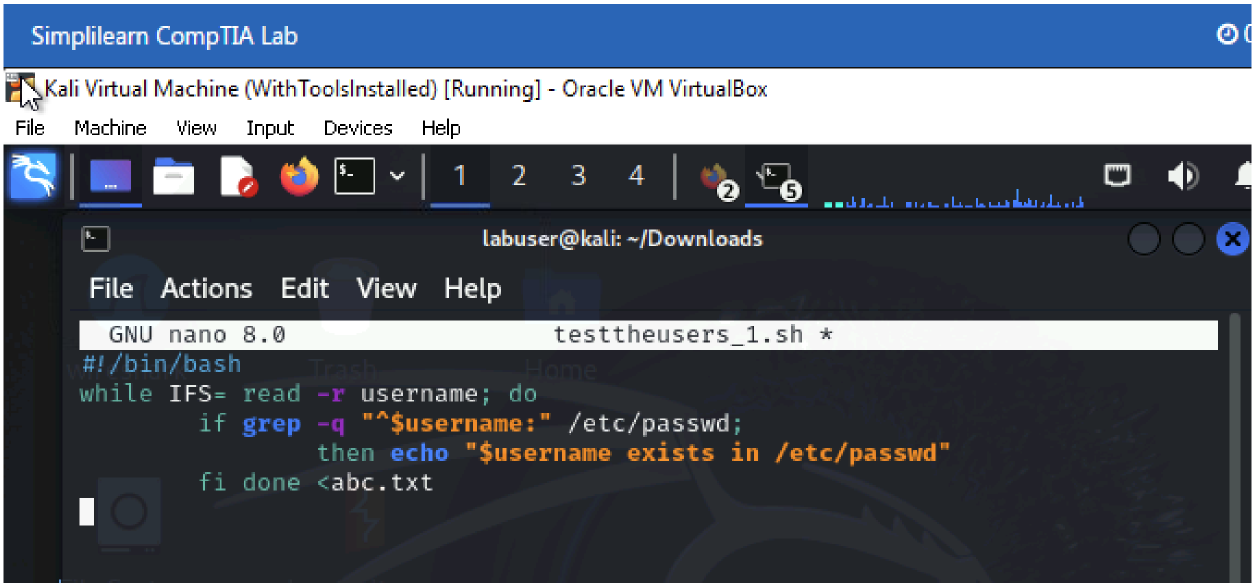
**nano testtheusers_1.sh**


Simplilearn CompTIA Lab
Kali Virtual Machine (WithToolsInstalled) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
labuser@kali: ~/Downloads
File Actions Edit View Help

```
  GNU nano 8.0                 testtheusers_1.sh
```

Step 2: Add the following script in the testtheusers_1.sh file

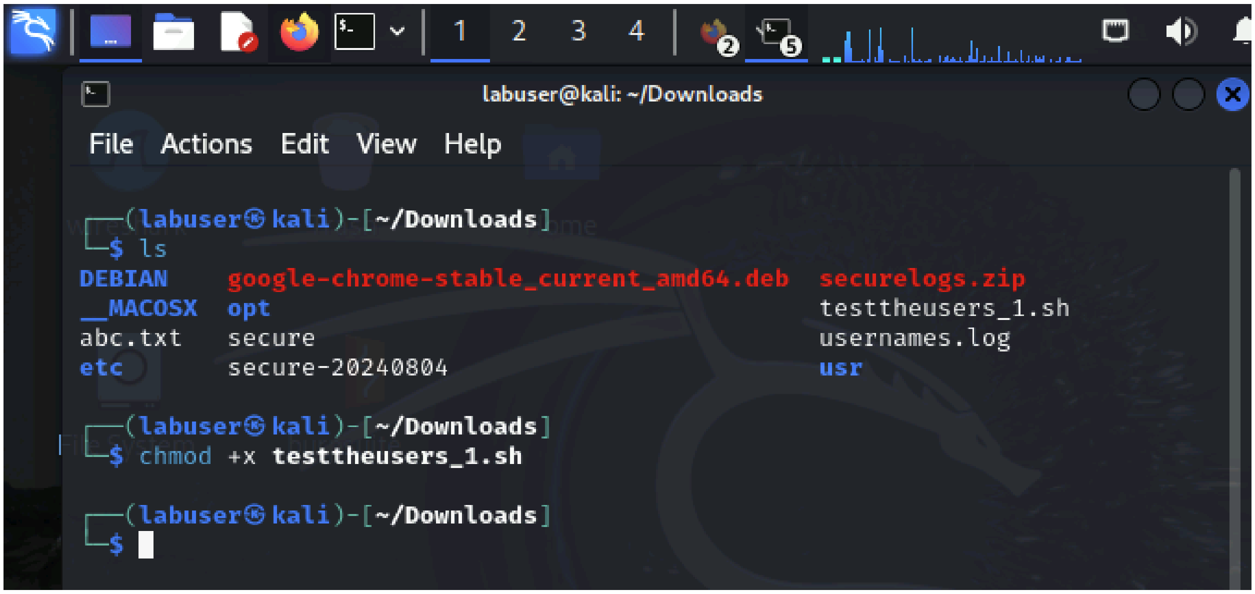
```
#!/bin/bash

while IFS= read -r username; do

        if grep -q "^$username:" /etc/passwd;

                then echo "$username exists in /etc/passwd"

        fi done <abc.txt
```


Simplilearn CompTIA Lab
Kali Virtual Machine (WithToolsInstalled) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
labuser@kali: ~/Downloads
File Actions Edit View Help

```
 GNU nano 8.0                     testtheusers_1.sh *
#!/bin/bash
while IFS= read -r username; do
        if grep -q "^$username:" /etc/passwd;
                then echo "$username exists in /etc/passwd"
        fi done <abc.txt
```

Step 3: Make the script executable by running the following command.

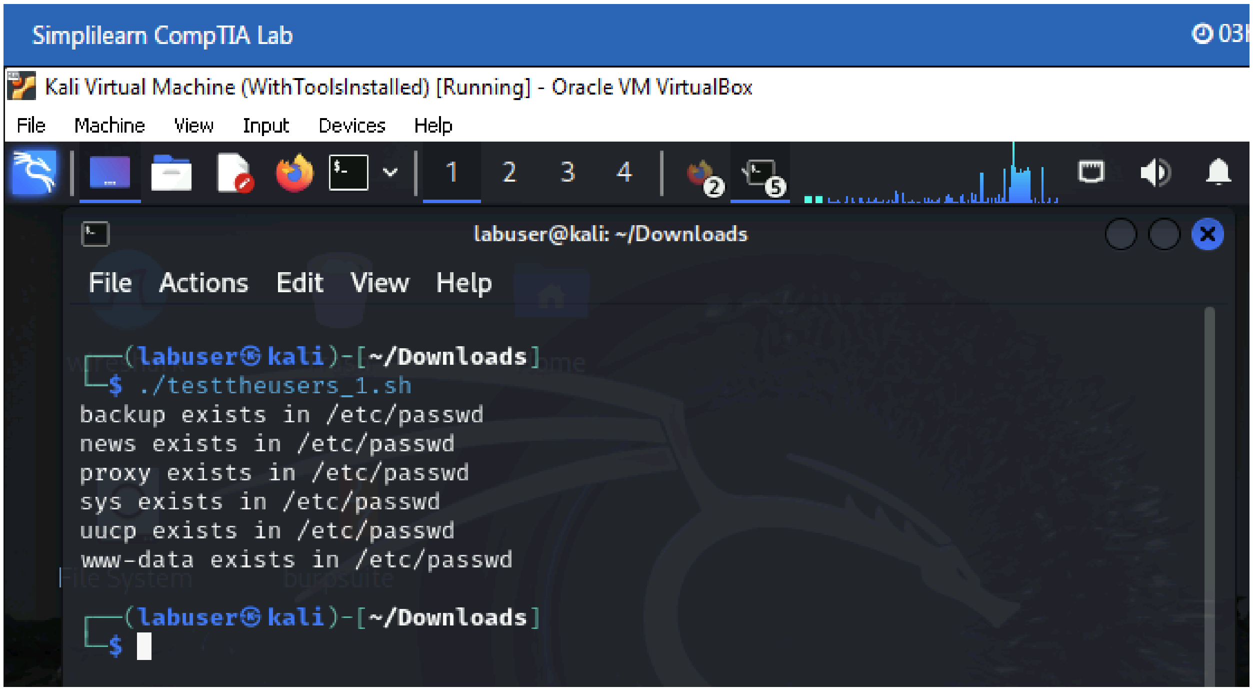
**chmod +x testtheusers_1.sh**



```
┌──(labuser㉿kali)-[~/Downloads]
└─$ ls
DEBIAN     google-chrome-stable_current_amd64.deb  securelogs.zip
__MACOSX   opt                                     testtheusers_1.sh
abc.txt    secure                                  usernames.log
etc        secure-20240804                         usr

┌──(labuser㉿kali)-[~/Downloads]
└─$ chmod +x testtheusers_1.sh

┌──(labuser㉿kali)-[~/Downloads]
└─$ 
```

Step 4: Run the following command to check the existence ofusernames in the system.

**./testtheusers_1.sh**



Simplilearn CompTIA Lab
03
Kali Virtual Machine (WithToolsInstalled) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
labuser@kali: ~/Downloads
File Actions Edit View Help

```
┌──(labuser㉿kali)-[~/Downloads]
└─$ ./testtheusers_1.sh
backup exists in /etc/passwd
news exists in /etc/passwd
proxy exists in /etc/passwd
sys exists in /etc/passwd
uucp exists in /etc/passwd
www-data exists in /etc/passwd

┌──(labuser㉿kali)-[~/Downloads]
└─$ 
```