

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.

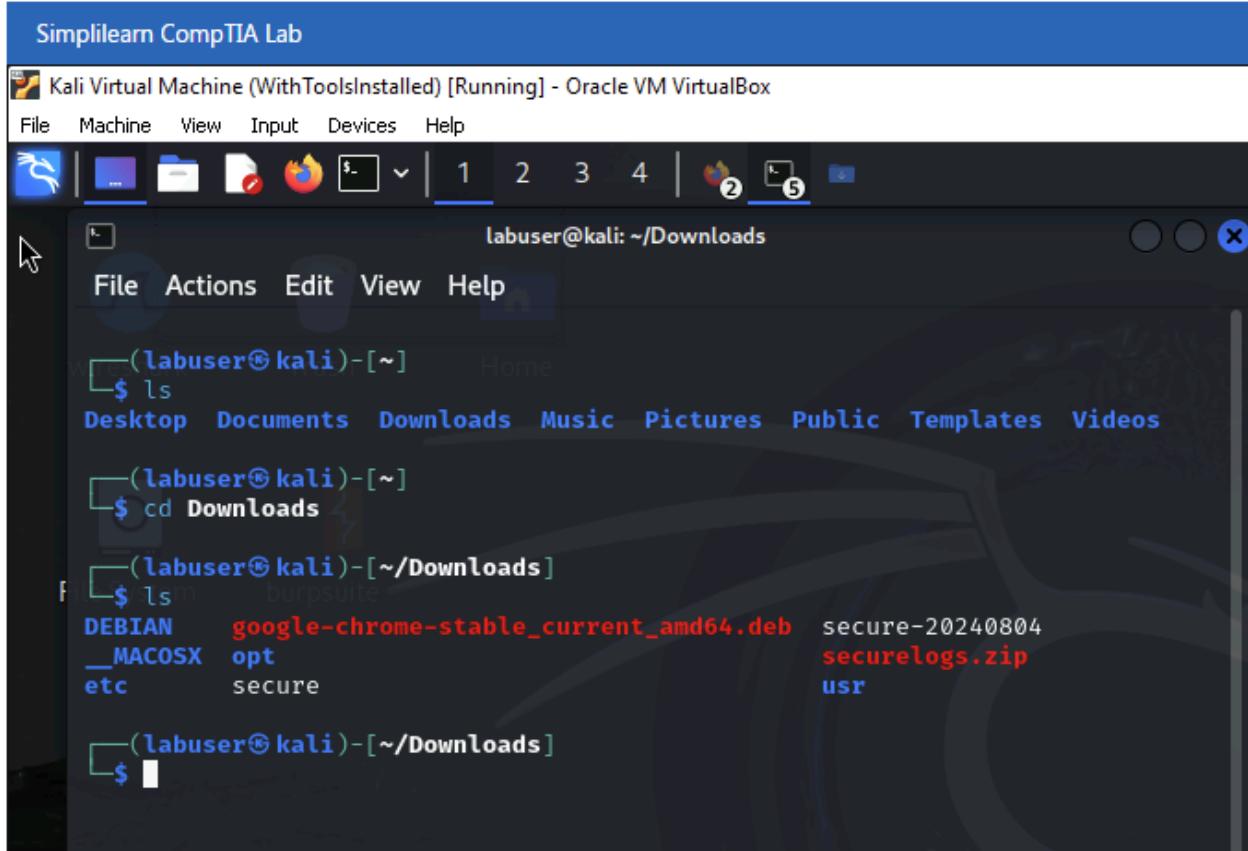
Tasks:

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.



The screenshot shows a terminal window titled "Simplilearn CompTIA Lab" running on a Kali Linux virtual machine. The terminal window has a dark theme with blue highlights. The title bar says "Simplilearn CompTIA Lab" and "Kali Virtual Machine (WithToolsInstalled) [Running] - Oracle VM VirtualBox". The menu bar includes File, Machine, View, Input, Devices, and Help. The toolbar contains icons for Home, File Manager, Terminal, and a browser. The terminal session shows the user's path: ~Downloads. The user runs the command "ls" to list the contents of the Downloads directory. The output shows several files and folders: DEBIAN, google-chrome-stable_current_amd64.deb, _MACOSX, opt, etc, secure, securelogs.zip, and usr. The "securelogs.zip" file is highlighted in red.

```
labuser@kali: ~/Downloads
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
$ cd Downloads
$ ls
DEBIAN      google-chrome-stable_current_amd64.deb  secure-20240804
_MACOSX    opt                                         securelogs.zip
etc        secure                                       usr
```

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

```
(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

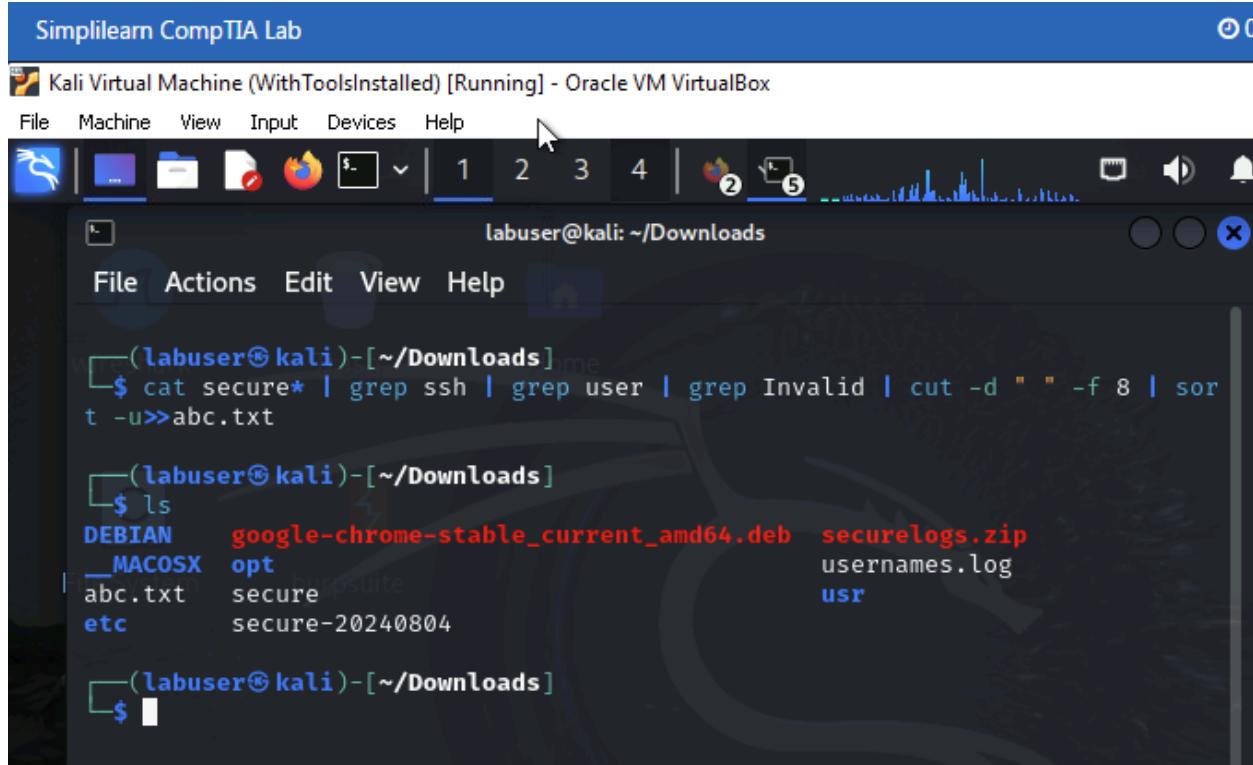
```
(labuser㉿kali)-[~/Downloads]
$ grep "Failed password for" secure* | grep -v "invalid user" | awk '{print $9}'>>usernames.log

(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
```



The screenshot shows a terminal window titled 'Simplilearn CompTIA Lab' running on a Kali Linux virtual machine. The terminal displays the following command being run:

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

After executing the command, the terminal shows the contents of the 'abc.txt' file:

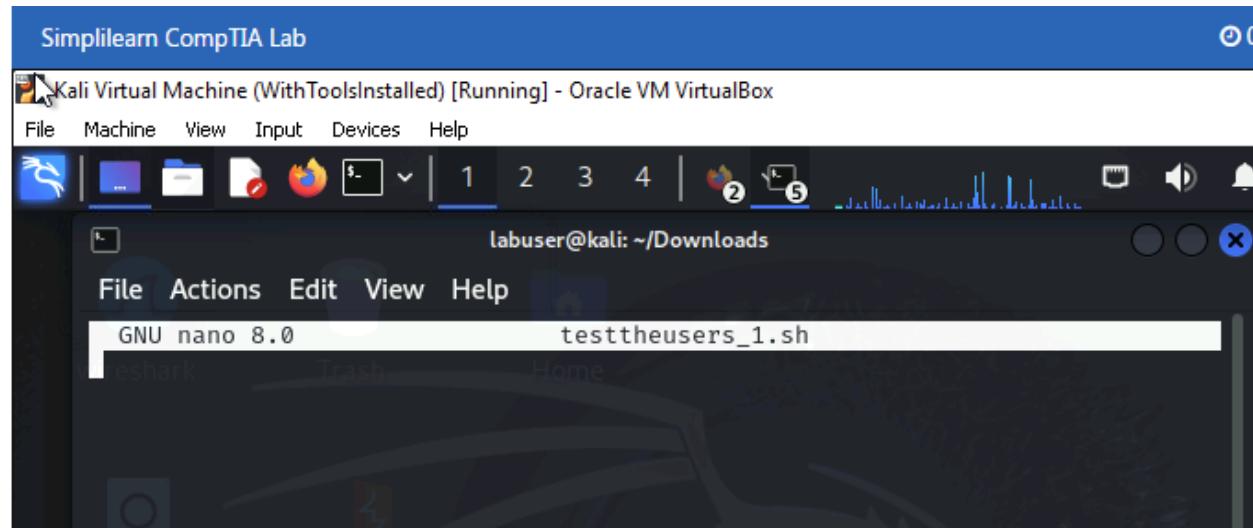
```
(labuser㉿kali)-[~/Downloads]$ ls
DEBIAN      google-chrome-stable_current_amd64.deb  securelogs.zip
__MACOSX    opt                           usernames.log
abc.txt     secure                         usr
etc        secure-20240804
```

The terminal prompt '\$' is visible at the bottom.

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
```



The screenshot shows a terminal window titled 'Simplilearn CompTIA Lab' running on a Kali Linux virtual machine. The terminal displays the command 'nano testtheusers_1.sh' being run:

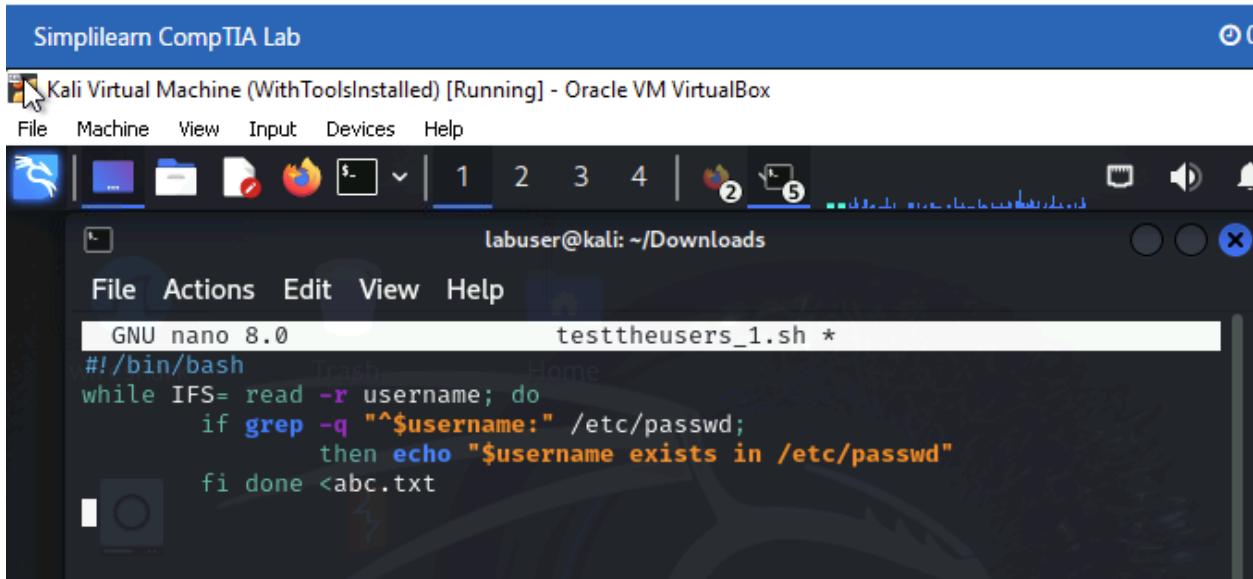
```
GNU nano 8.0          testtheusers_1.sh
```

The terminal prompt '\$' is visible at the bottom.

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

```
#!/bin/bash

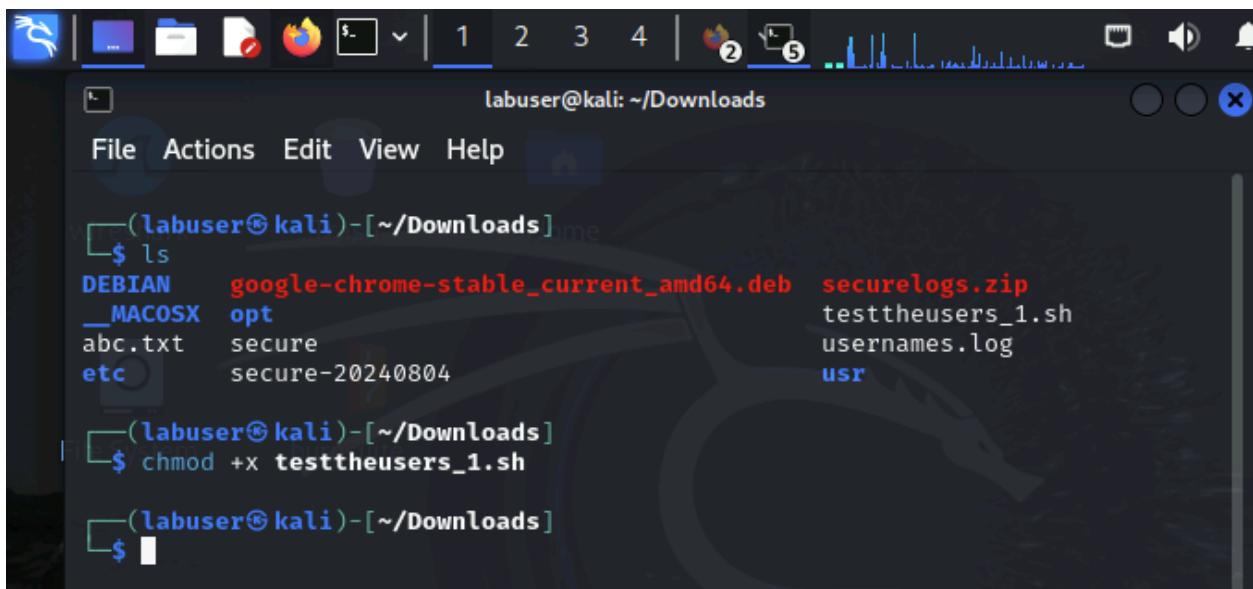
while IFS= read -r username; do
    if grep -q "^$username:" /etc/passwd;
        then echo "$username exists in /etc/passwd"
    fi done <abc.txt
```



The screenshot shows a terminal window titled "Simplilearn CompTIA Lab" running on a Kali Linux virtual machine. The window title bar says "Kali Virtual Machine (WithToolsInstalled) [Running] - Oracle VM VirtualBox". The terminal window has a dark theme with a blue header bar. The command "GNU nano 8.0" is displayed at the top, followed by the script content. The script uses "#!/bin/bash" as the shebang, a "while" loop to read from "abc.txt", and a "grep" command to check if the username exists in "/etc/passwd". The terminal prompt "labuser@kali: ~/Downloads" is visible at the bottom.

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

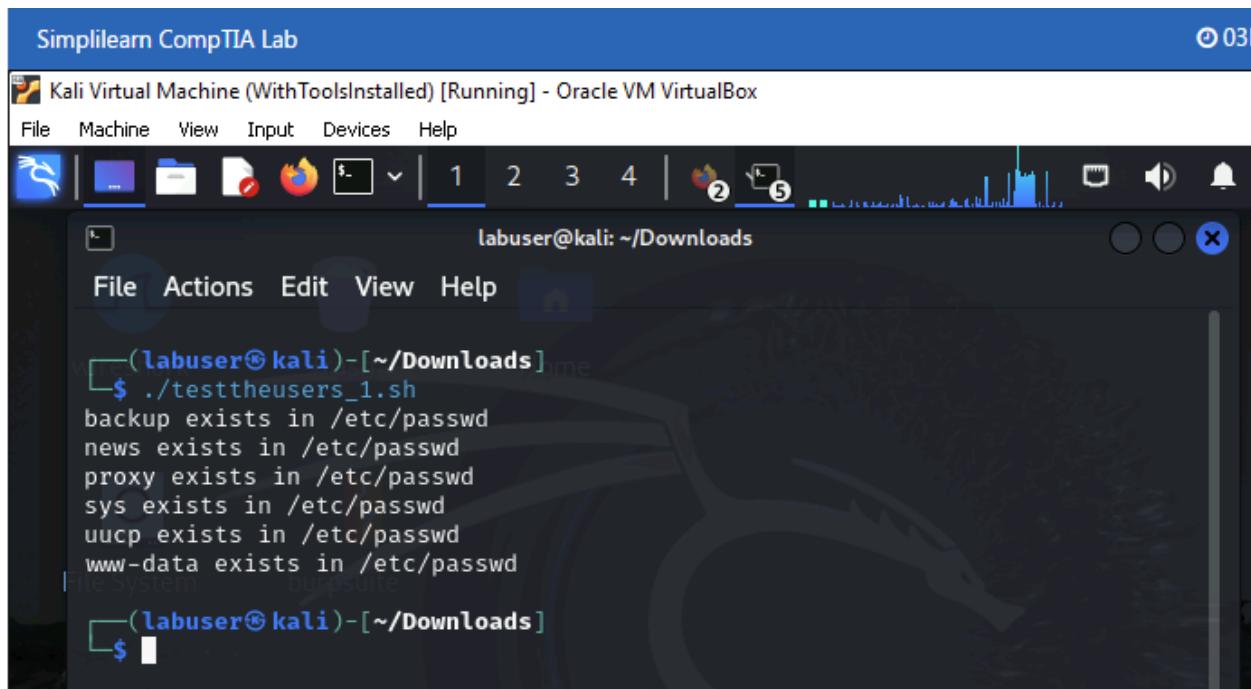
```
chmod +x testtheusers_1.sh
```



The screenshot shows a terminal window titled "(labuser㉿kali)-[~/Downloads]" running on a Kali Linux virtual machine. The terminal window has a light blue header bar. The command "ls" is run, listing files in the current directory: abc.txt, secure, etc, google-chrome-stable_current_amd64.deb, securelogs.zip, testtheusers_1.sh, usernames.log, and usr. Below this, the command "chmod +x testtheusers_1.sh" is run to make the script executable. The terminal prompt "labuser@kali: ~/Downloads" is visible at the bottom.

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

./testtheusers_1.sh



The screenshot shows a terminal window titled "Simplilearn CompTIA Lab" running on a Kali Linux virtual machine. The window title bar also indicates it's a "Kali Virtual Machine (WithToolsInstalled) [Running] - Oracle VM VirtualBox". The terminal window has tabs labeled 1, 2, 3, 4, and 5, with tab 5 currently active. The prompt is "labuser@kali: ~/Downloads". The terminal displays the output of the script:

```
(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]$
```