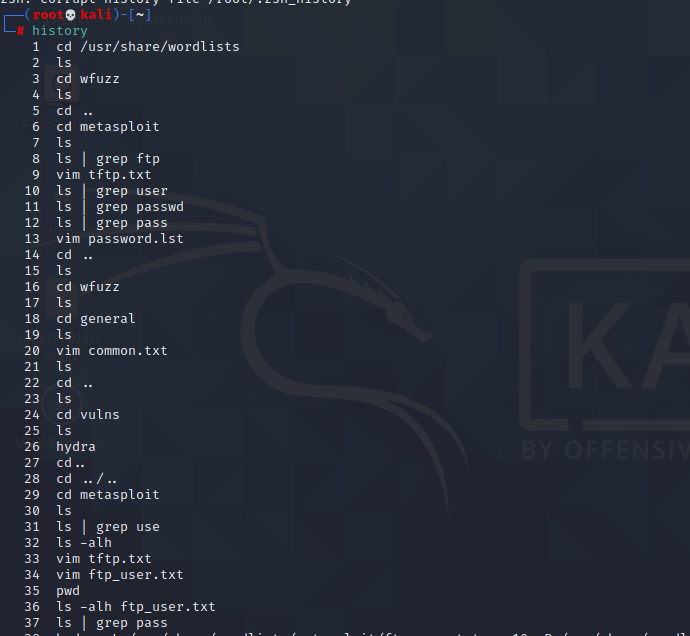
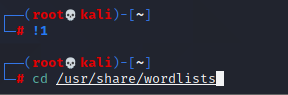
**3.1.3.2 Exercises**

1. Inspect your bash history and use history expansion to re-run a command from it.

use history

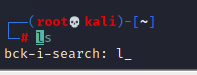


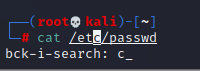
and select command

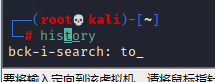


2. Execute different commands of your choice and experiment browsing the history through

the shortcuts as well as the reverse-i-search facility.



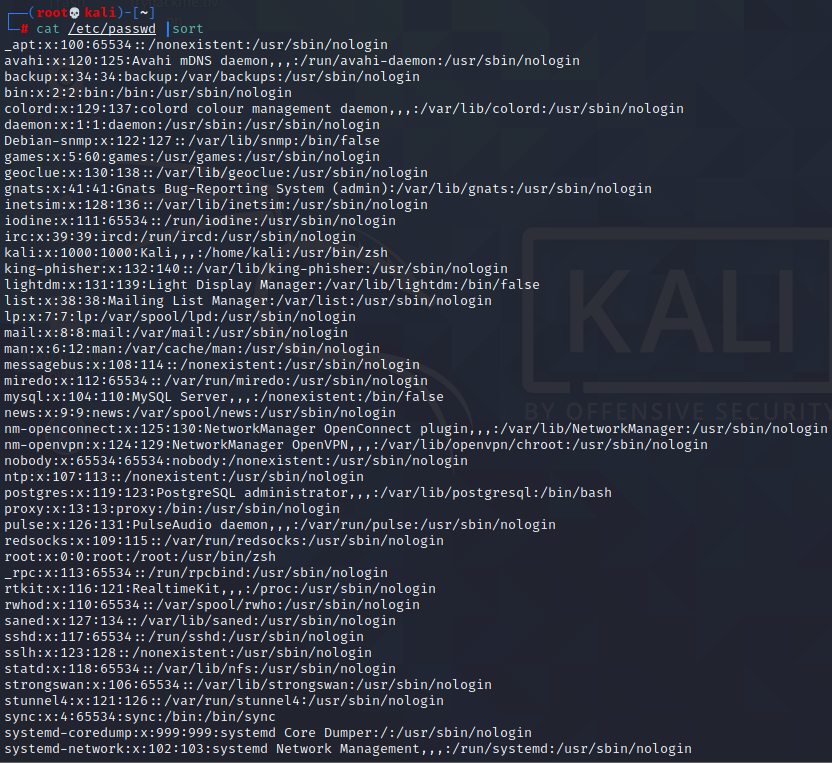




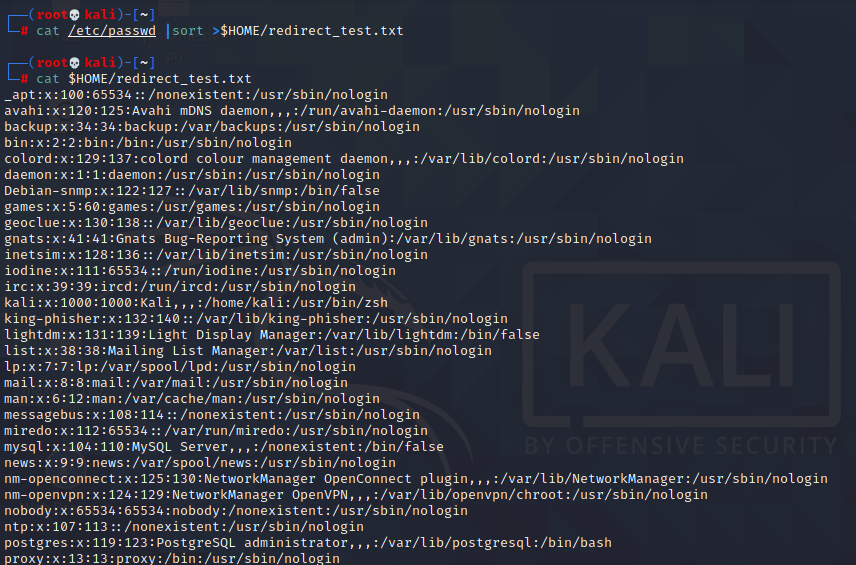
**3.2.5.1 Exercises**

1. Use the cat command in conjunction with sort to reorder the content of the /etc/passwd

file on your Kali Linux system.



1. Redirect the output of the previous exercise to a file of your choice in your home directory.



**3.3.5.1 Exercises**

1. Using /etc/passwd , extract the user and home directory fields for all users on your Kali

machine for which the shell is set to /bin/false. Make sure you use a Bash one-liner to print

the output to the screen. The output should look similar to Listing 53 below:

kali@kali:~$ YOUR COMMAND HERE...

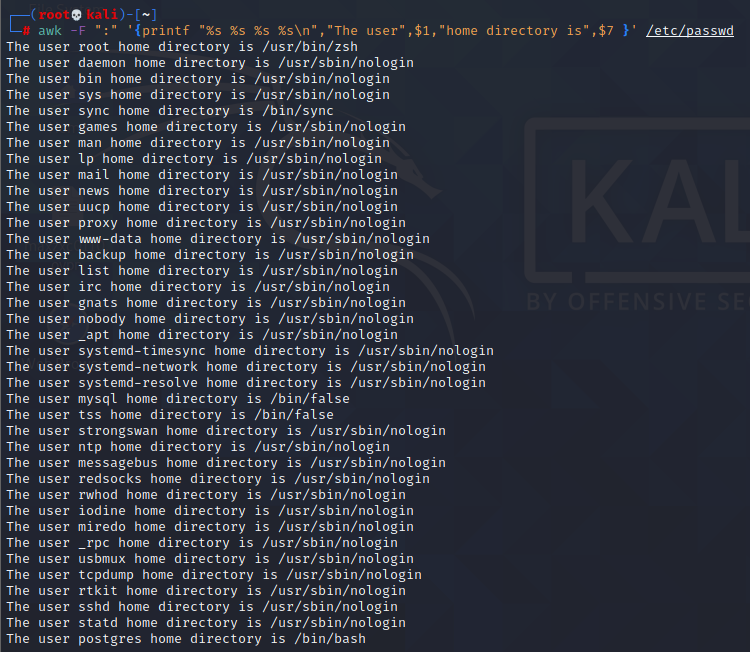
The user mysql home directory is /nonexistent

The user Debian-snmp home directory is /var/lib/snmp

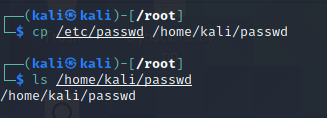
The user speech-dispatcher home directory is /var/run/speech-dispatcher

The user Debian-gdm home directory is /var/lib/gdm3

Listing 53 - Home directories for users with /bin/false shells

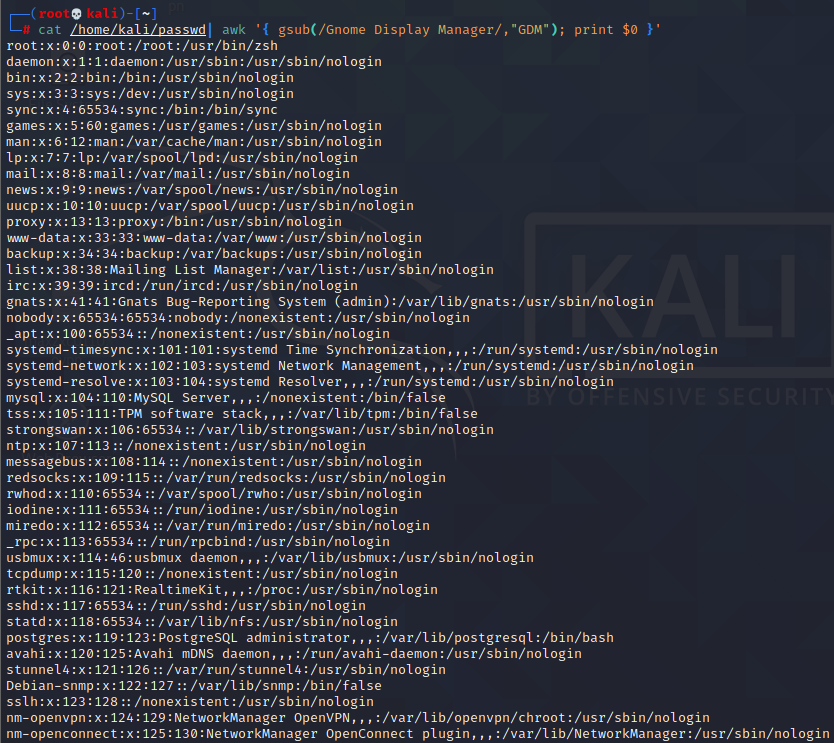


1. Copy the /etc/passwd file to your home directory ( /home/kali ).



3. Use cat in a one-liner to print the output of the /kali/passwd and replace all instances of the

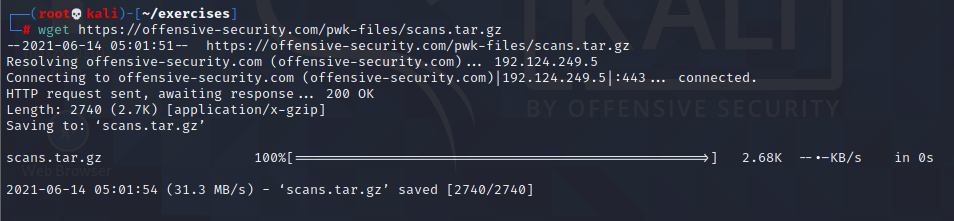
“Gnome Display Manager” string with “GDM”.



**3.5.3.1 Exercises**

1. Download the archive from the following URL https://offensive-security.com/pwk-

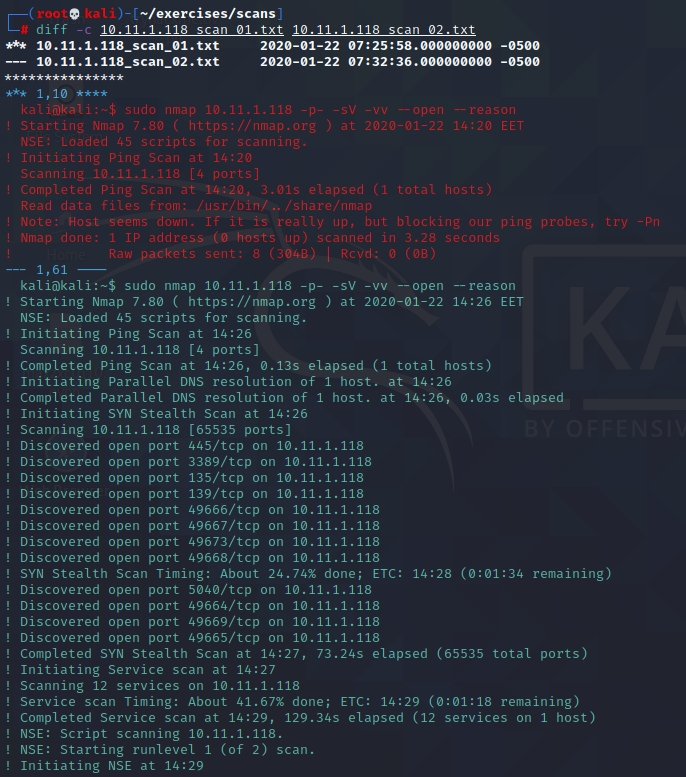
files/scans.tar.gz



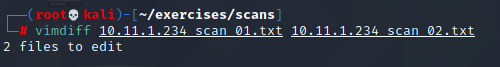
2. This archive contains the results of scanning the same target machine at different times.

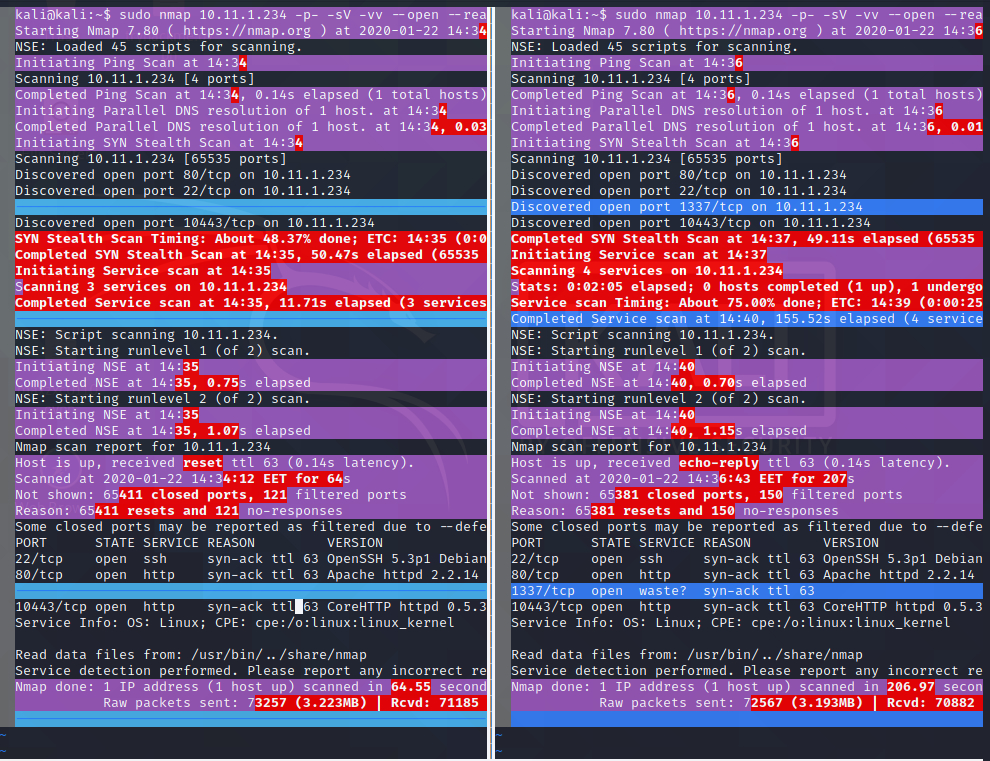
Extract the archive and see if you can spot the differences by diffing the scans.

use diff

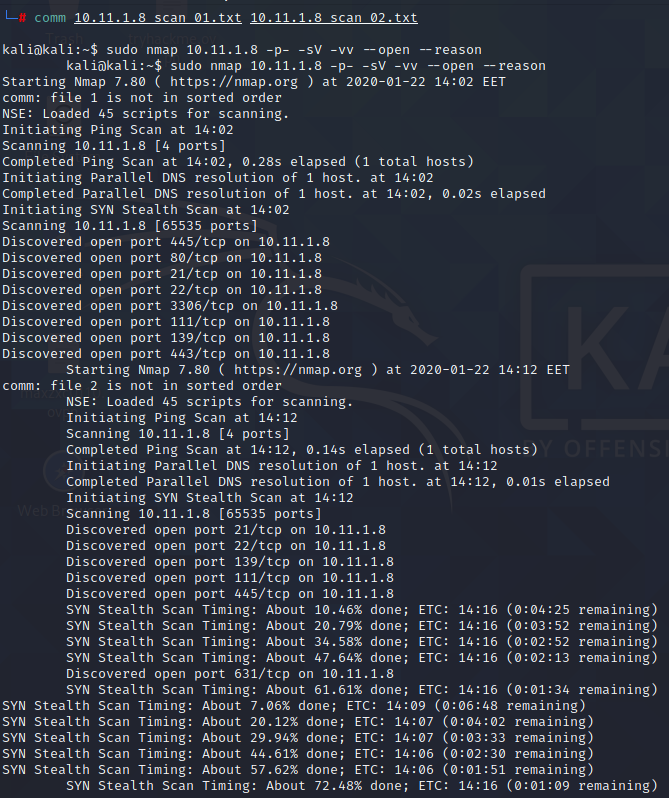


use vimdiff





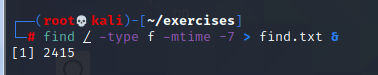
use comm



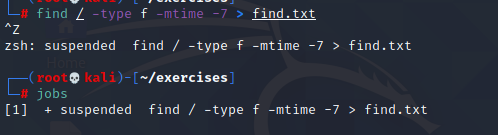
**3.6.3.1 Exercises**

1. Find files that have changed on your Kali virtual machine within the past 7 days by running a

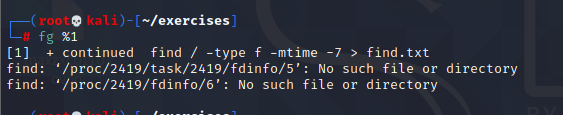
specific command in the background.



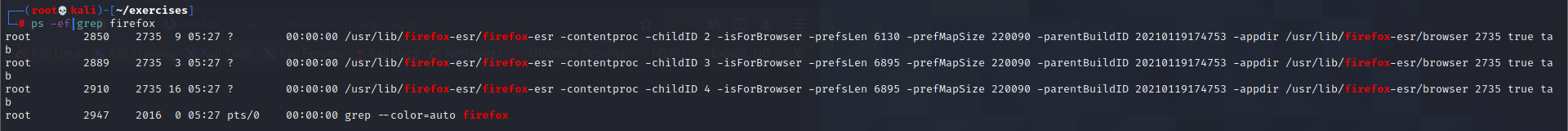
1. Re-run the previous command and suspend it; once suspended, background it.



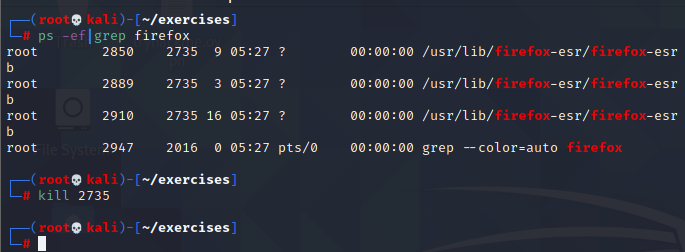
1. Bring the previous background job into the foreground.



1. Start the Firefox browser on your Kali system. Use ps and grep to identify Firefox’s PID.



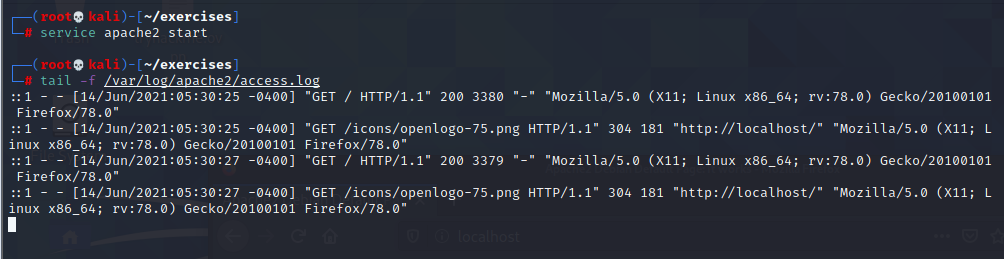
1. Terminate Firefox from the command line using its PID.



**3.7.2.1 Exercises**

1. Start your apache2 web service and access it locally while monitoring its access.log file in

real-time.

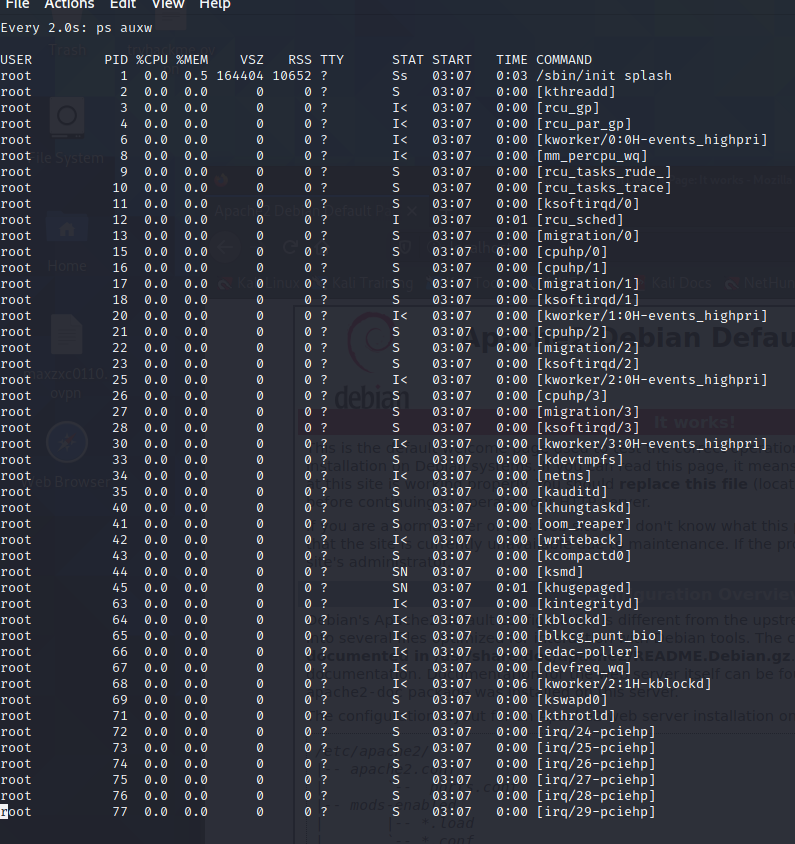


2. Use a combination of watch and ps to monitor the most CPU-intensive processes on your

Kali machine in a terminal window; launch different applications to see how the list changes

in real time.



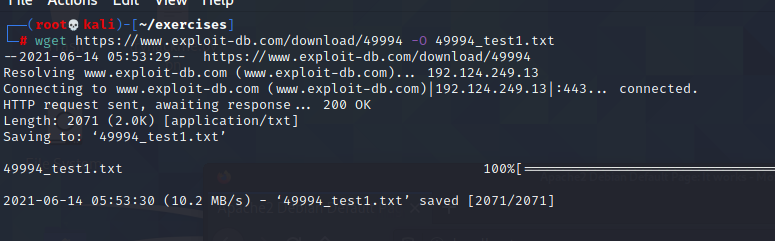


**3.8.3.1 Exercise**

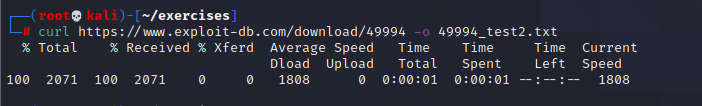
1. Download the PoC code for an exploit from https://www.exploit-db.com using curl , wget ,

and axel , saving each download with a different name.

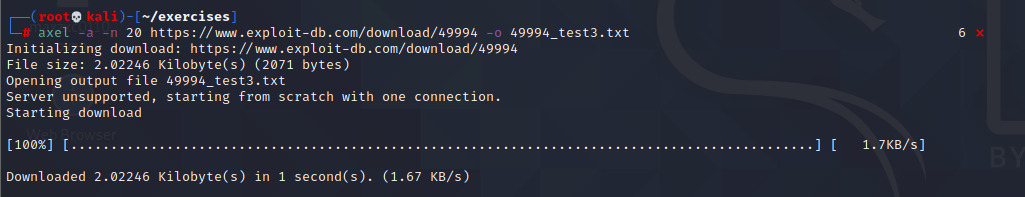
wget



curl



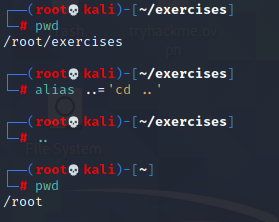
axel



**3.9.3.1 Exercises**

1. Create an alias named “..” to change to the parent directory and make it persistent across

terminal sessions.



2. Permanently configure the history command to store 10000 entries and include the full date

in its output.

