Task 2: Kali Linux – Hands on

1. Objective:

Practice Linux commands from basic to Advanced levels, install Kali Linux tools from GitHub, and perform a specific attack using one of the tools.

Steps to Complete the Task:

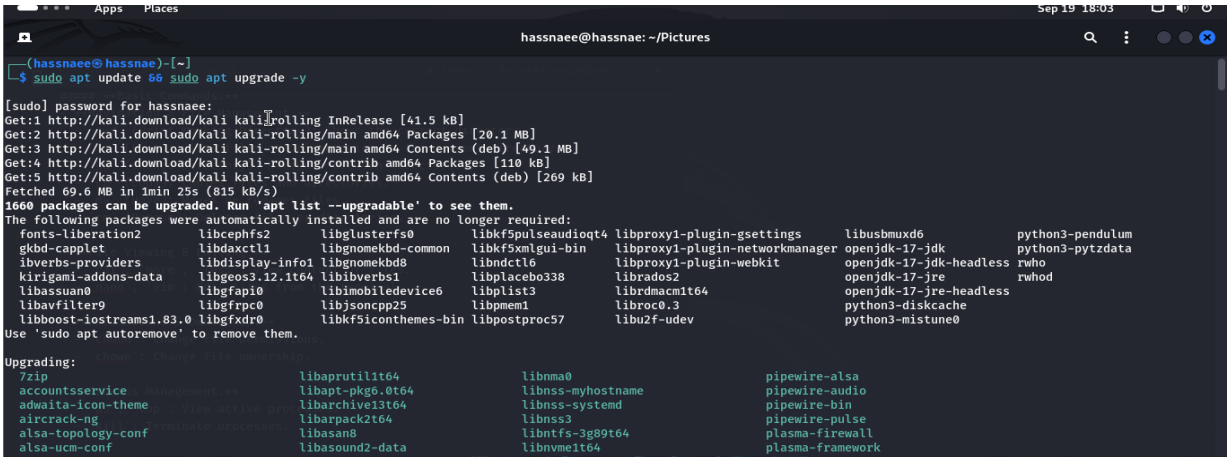
1. Install Kali Linux:

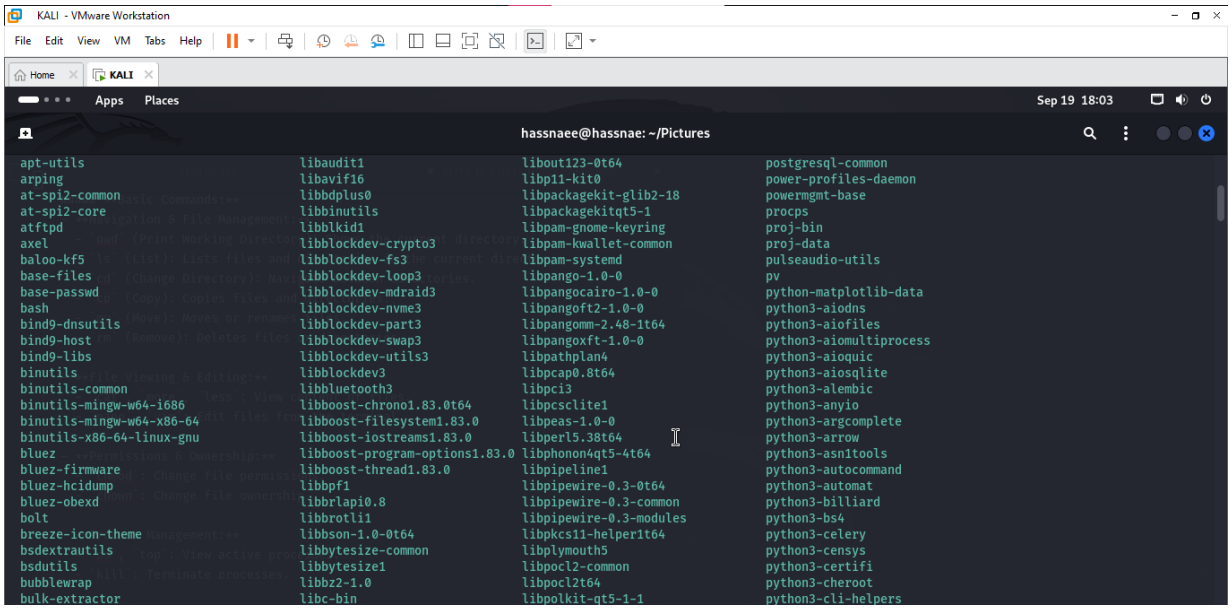
- Download the Kali Linux ISO from the official website: **Kali Linux Download.**
- Install Kali Linux either on a physical machine, in a virtual environment (using VMware or VirtualBox), or as a dual boot with another OS.

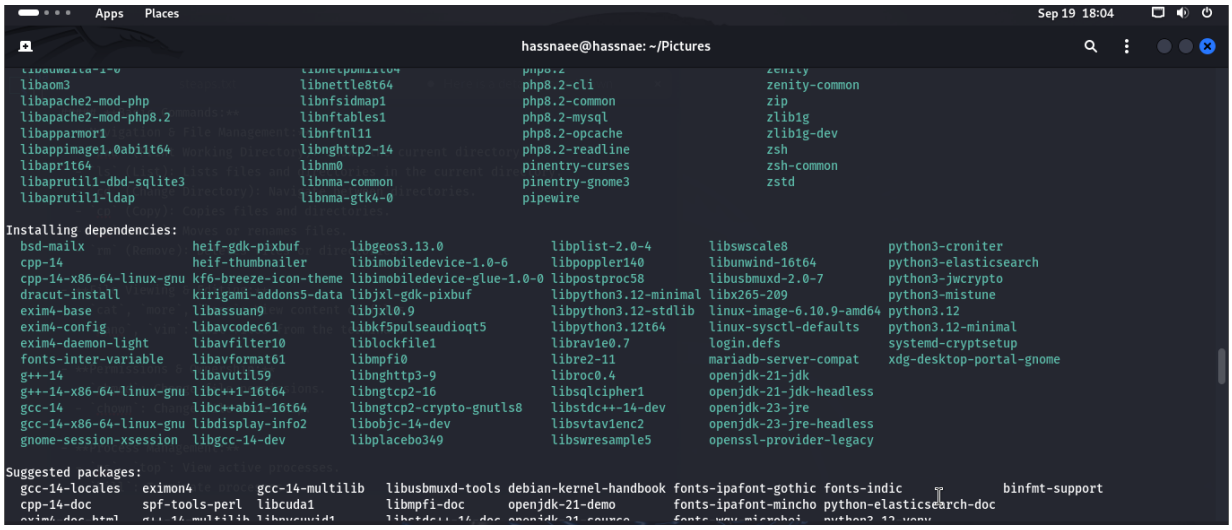
##**(**this steps is already done)

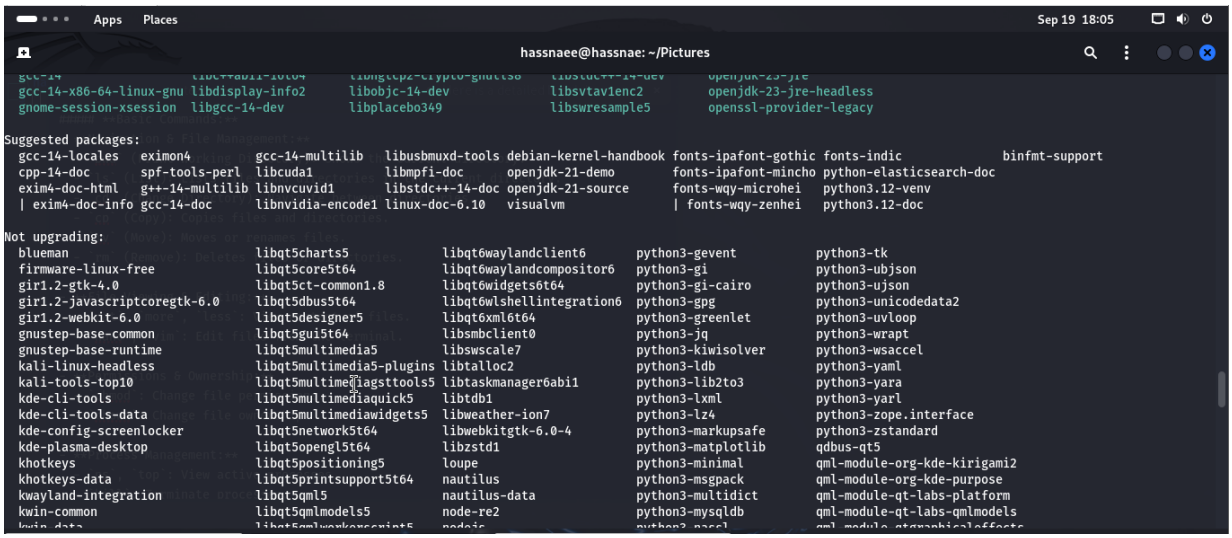
After installation, we need to make sure to update the system by running:

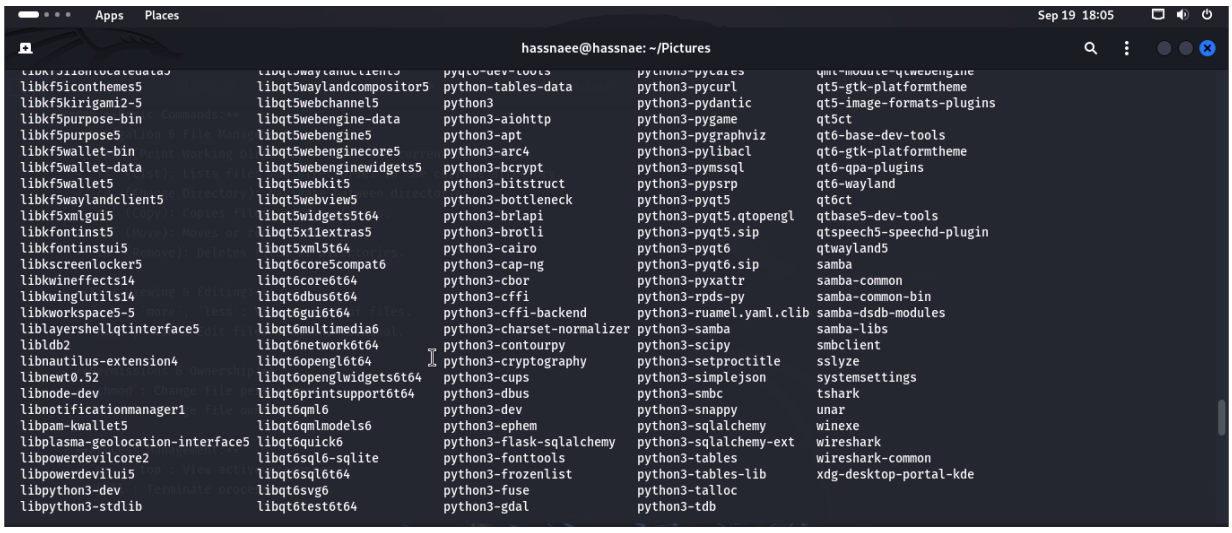
sudo apt update && sudo apt upgrade -y






Apps Places
Sep 19 18:04
hassnaee@hassnae: ~/Pictures
libaom3 libnettle8t64 php8.2-cli zenity-common
libapache2-mod-php libnfsidmap1 php8.2-common zip
libapache2-mod-php8.2 libnftables1 php8.2-mysql zlib1g
libapparmor1 libnftnl11 php8.2-opcache zlib1g-dev
libappimage1.0abi1t64 libnghttp2-14 php8.2-readline zsh
libapr1t64 libnm0 pinentry-curses zsh-common
libaprutil1-dbd-sqlite3 libnma-common pinentry-gnome3 zstd
libaprutil1-ldap libnma-gtk4-0 pipewire
Installing dependencies:
bsd-mailx heif-gdk-pixbuf libgeos3.13.0 libplist-2.0-4 libswscale8 python3-croniter
cpp-14 heif-thumbnailer libimobiledevice-1.0-6 libpoppler140 libunwind-16t64 python3-elasticsearch
cpp-14-x86-64-linux-gnu kf6-breeze-icon-theme libimobiledevice-glue-1.0-0 libpostproc58 libusbmuxd-2.0-7 python3-jwcrypto
dracut-install kirigami-addons5-data libjxl-gdk-pixbuf libpython3.12-minimal libx265-209 python3-mistune
exim4-base libassuan9 libjxl0.9 libpython3.12-stdlib linux-image-6.10.9-amd64 python3.12
exim4-config libavcodec61 libkf5pulseaudioqt5 libpython3.12t64 linux-sysctl-defaults python3.12-minimal
exim4-daemon-light libavfilter10 liblockfile1 libravle0.7 login.defs systemd-cryptsetup
fonts-inter-variable libavformat61 libmpfi0 libre2-11 mariadb-server-compat xdg-desktop-portal-gnome
g++-14 libavutil59 libnghttp3-9 libroc0.4 openjdk-21-jdk
g++-14-x86-64-linux-gnu libc++1-16t64 libngtcp2-16 libsqlcipher1 openjdk-21-jdk-headless
gcc-14 libc++abi1-16t64 libngtcp2-crypto-gnutls8 libstdc++-14-dev openjdk-23-jre
gcc-14-x86-64-linux-gnu libdisplay-info2 libobjc-14-dev libsvtav1enc2 openjdk-23-jre-headless
gnome-session-xsession libgcc-14-dev libplacebo349 libswresample5 openssl-provider-legacy
Suggested packages:
gcc-14-locales exim4 gcc-14-multilib libusbmuxd-tools debian-kernel-handbook fonts-ipafont-gothic fonts-indic binfmt-support
cpp-14-doc spf-tools-perl libcuda1 libmpfi-doc openjdk-21-demo fonts-ipafont-mincho python-elasticsearch-doc


Apps Places
Sep 19 18:05
hassnaee@hassnae: ~/Pictures
gcc-14-x86-64-linux-gnu libdisplay-info2 libobjc-14-dev libsvtav1enc2 openjdk-23-jre-headless
gnome-session-xsession libgcc-14-dev libplacebo349 libswresample5 openssl-provider-legacy
Suggested packages:
gcc-14-locales exim4 gcc-14-multilib libusbmuxd-tools debian-kernel-handbook fonts-ipafont-gothic fonts-indic binfmt-support
cpp-14-doc spf-tools-perl libcuda1 libmpfi-doc openjdk-21-demo fonts-ipafont-mincho python-elasticsearch-doc
exim4-doc-html g++-14-multilib libnvcuvid1 libstdc++-14-doc openjdk-21-source fonts-wqy-microhei python3.12-venv
| exim4-doc-info gcc-14-doc libnvidia-encode1 linux-doc-6.10 visualvm | fonts-wqy-zenhei python3.12-doc
Not upgrading:
blueman libqt5charts5 libqt6waylandclient6 python3-gevent python3-tk
firmware-linux-free libqt5core5t64 libqt6waylandcompositor6 python3-gi python3-ubjson
gir1.2-gtk-4.0 libqt5ct-common1.8 libqt6widgets6t64 python3-gi-cairo python3-ujson
gir1.2-javascriptcoregtk-6.0 libqt5dbus5t64 libqt6wlshellintegration6 python3-gpg python3-unicodedata2
gir1.2-webkit-6.0 libqt5designer5 libqt6xml6t64 python3-greenlet python3-uvloop
gnustep-base-common libqt5gui5t64 libsmbclient0 python3-jq python3-wrapt
gnustep-base-runtime libqt5multimedia5 libswscale7 python3-kiwisolver python3-wsaccel
kali-linux-headless libqt5multimedia5-plugins libtalloc2 python3-ldb python3-yaml
kali-tools-top10 libqt5multimediagsttools5 libtaskmanager6abi1 python3-lib2to3 python3-yara
kde-cli-tools libqt5multimediaquick5 libtdb1 python3-lxml python3-yarl
kde-cli-tools-data libqt5multimediawidgets5 libweather-ion7 python3-lz4 python3-zope.interface
kde-config-screenlocker libqt5network5t64 libwebkitgtk-6.0-4 python3-markupsafe python3-zstandard
kde-plasma-desktop libqt5opengl5t64 libzstd1 python3-matplotlib qdbus-qt5
khotkeys libqt5positioning5 loupe python3-minimal qml-module-org-kde-kirigami2
khotkeys-data libqt5printsupport5t64 nautilus python3-msgpack qml-module-org-kde-purpose
kwayland-integration libqt5qml5 nautilus-data python3-multidict qml-module-qt-labs-platform
kwin-common libqt5qmlmodels5 node-re2 python3-mysqldb qml-module-qt-labs-qmlmodels


Apps Places
Sep 19 18:05
hassnaee@hassnae: ~/Pictures
libkf5iconthemes5 libqt5waylandcompositor5 python-tables-data python3-pycurl qt5-gtk-platformtheme
libkf5kirigami2-5 libqt5webchannel5 python3 python3-pydantic qt5-image-formats-plugins
libkf5purpose-bin libqt5webengine-data python3-aiohttp python3-pygame qt5ct
libkf5purpose5 libqt5webengine5 python3-apt python3-pygraphviz qt6-base-dev-tools
libkf5wallet-bin libqt5webenginecore5 python3-arc4 python3-pylibacl qt6-gtk-platformtheme
libkf5wallet-data libqt5webenginewidgets5 python3-bcrypt python3-pymssql qt6-qpa-plugins
libkf5wallet5 libqt5webkit5 python3-bitstruct python3-pypsrp qt6-wayland
libkf5waylandclient5 libqt5webview5 python3-bottleneck python3-pyqt5 qt6ct
libkf5xmlgui5 libqt5widgets5t64 python3-brlapi python3-pyqt5.qtopengl qtbase5-dev-tools
libkfontinst5 libqt5x11extras5 python3-brotli python3-pyqt5.sip qtspeech5-speechd-plugin
libkfontinstui5 libqt5xml5t64 python3-cairo python3-pyqt6 qtwayland5
libkscreenlocker5 libqt6core5compat6 python3-cap-ng python3-pyqt6.sip samba
libkwineffects14 libqt6core6t64 python3-cbor python3-pyxattr samba-common
libkwinglutils14 libqt6dbus6t64 python3-cffi python3-rpds-py samba-common-bin
libkworkspace5-5 libqt6gui6t64 python3-cffi-backend python3-ruamel.yaml.clib samba-dsdb-modules
liblayershellqtinterface5 libqt6multimedia6 python3-charset-normalizer python3-samba samba-libs
libldb2 libqt6network6t64 python3-contourpy python3-scipy smbclient
libnautilus-extension4 libqt6opengl6t64 python3-cryptography python3-setproctitle sslyze
libnewt0.52 libqt6openglwidgets6t64 python3-cups python3-simplejson systemsettings
libnode-dev libqt6printsupport6t64 python3-dbus python3-smbc tshark
libnotificationmanager1 libqt6qml6 python3-dev python3-snappy unar
libpam-kwallet5 libqt6qmlmodels6 python3-ephem python3-sqlalchemy winexe
libplasma-geolocation-interface5 libqt6quick6 python3-flask-sqlalchemy python3-sqlalchemy-ext wireshark
libpowerdevilcore2 libqt6sql6-sqlite python3-fonttools python3-tables wireshark-common
libpowerdevilui5 libqt6sql6t64 python3-frozenlist python3-tables-lib xdg-desktop-portal-kde
libpython3-dev libqt6svg6 python3-fuse python3-talloc
libpython3-stdlib libqt6test6t64 python3-gdal python3-tdb

2. Practice Basic to Advanced Linux Commands:

We start by familiarizing with essential Linux commands. Here are categories of commands that we should practice:

Basic Commands:

- **Navigation & File Management:**
  - pwd (Print Working Directory): Shows the current directory.
  - ls (List): Lists files and directories in the current directory.
  - cd (Change Directory): Navigate between directories.
  - cp (Copy): Copies files and directories.
  - mv (Move): Moves or renames files.
  - rm (Remove): Deletes files or directories.
- **File Viewing & Editing:**
  - cat, more, less: View content of files.
  - nano, vim: Edit files from the terminal.
- **Permissions & Ownership:**
  - Chmod: Change file permissions.
  - Chown: Change file ownership.
- **Process Management:**
  - ps, top: View active processes.
  - Kill: Terminate processes.

Intermediate Commands:

- **Networking:**
  - ifconfig or ip a: Check network configuration.
  - ping: Test network connectivity.
  - netstat: Check open ports and network connections.
- **System Information:**
  - df -h: Check disk space usage.
  - free -h: Check memory usage.
  - uname -a: View system information.
- **Archiving & Compression:**
  - tar, gzip, gunzip: Archive and compress files.

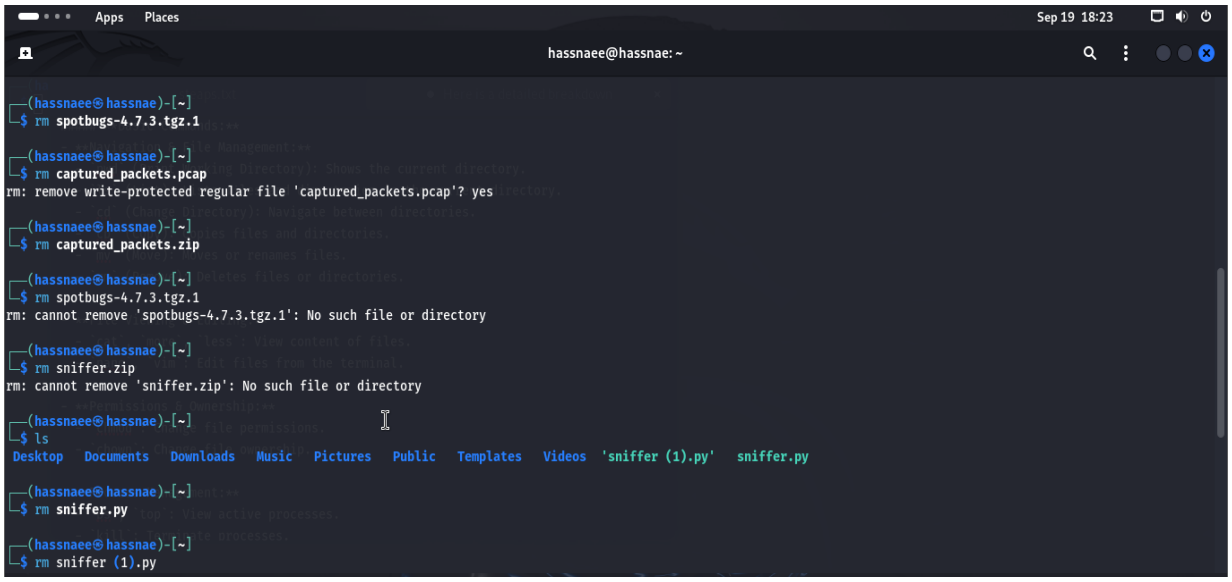
Advanced Commands:

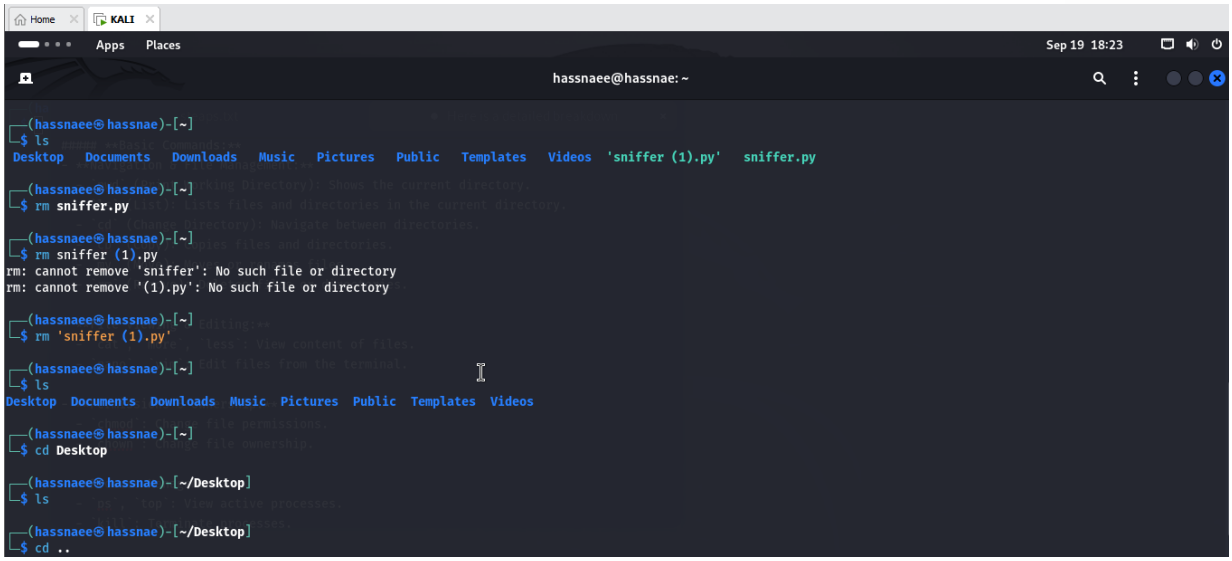
- **Scripting:**
  - Write and execute simple shell scripts (.sh).
- **Firewall & Security:**
  - ufw: Manage the firewall.
  - iptables: Advanced network traffic control.

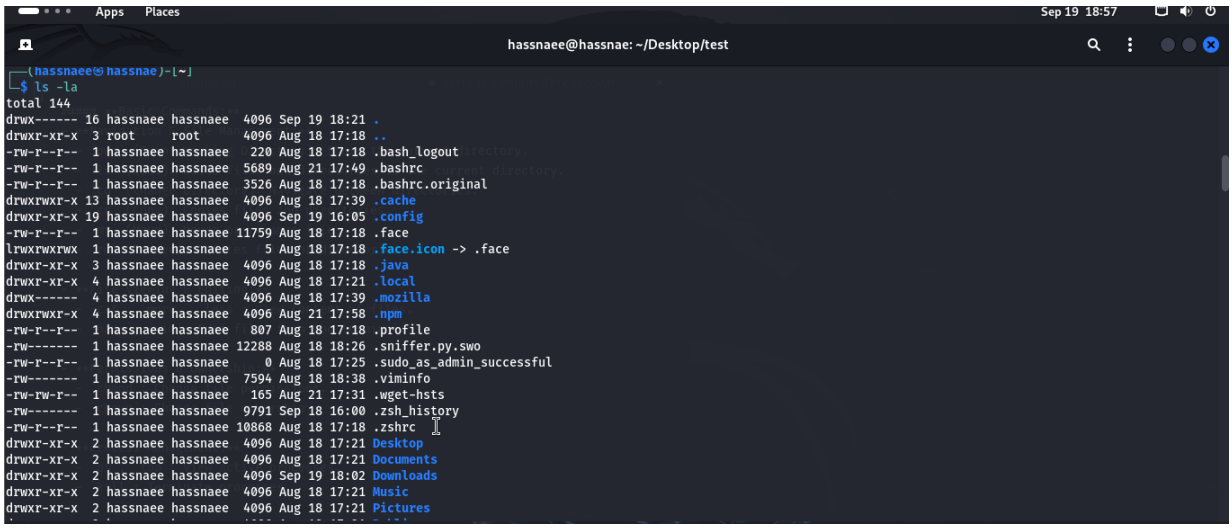
- **User Management:**
  - useradd, passwd, usermod, userdel: Manage users.
  - groupadd, groupdel, gpasswd: Manage groups.


hassnaee@hassnae: ~
Desktop Downloads Pictures Templates captured_packets.pcap 'sniffer (1).py' sniffer.zip spotbugs-4.7.3.tgz
Documents Music Public Videos captured_packets.zip sniffer.py sniffer_assignment.zip spotbugs-4.7.3.tgz.1
rm: cannot remove 'sniffer': No such file or directory
rm: cannot remove '(1).py': No such file or directory
[sudo] password for hassnaee:


hassnaee@hassnae: ~
rm: remove write-protected regular file 'captured_packets.pcap'? yes
rm: cannot remove 'spotbugs-4.7.3.tgz.1': No such file or directory
rm: cannot remove 'sniffer.zip': No such file or directory

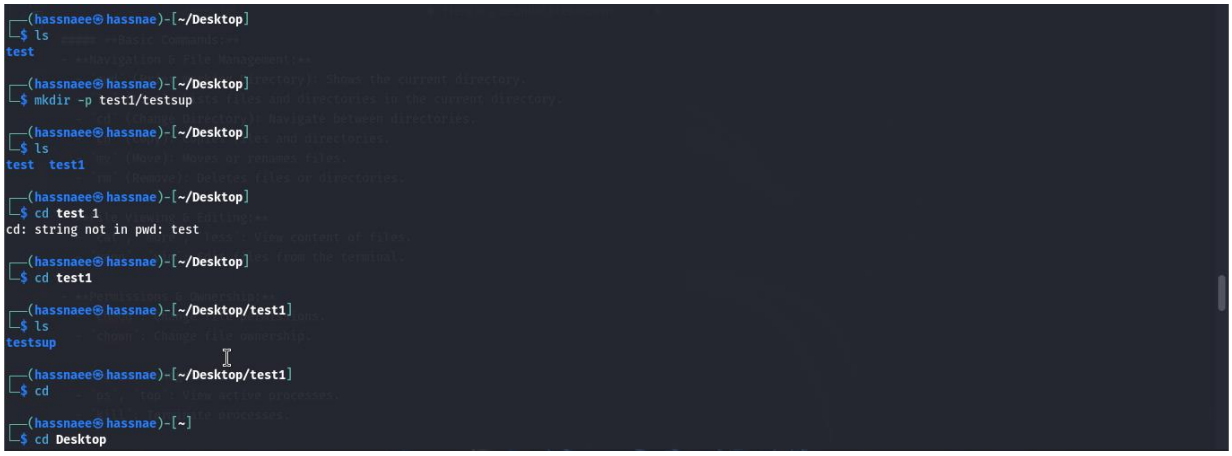

Apps Places
Sep 19 18:23
hassnaee@hassnae: ~
rm: remove write-protected regular file 'captured_packets.pcap'? yes
rm: cannot remove 'spotbugs-4.7.3.tgz.1': No such file or directory
rm: cannot remove 'sniffer.zip': No such file or directory
Desktop Documents Downloads Music Pictures Public Templates Videos 'sniffer (1).py' sniffer.py

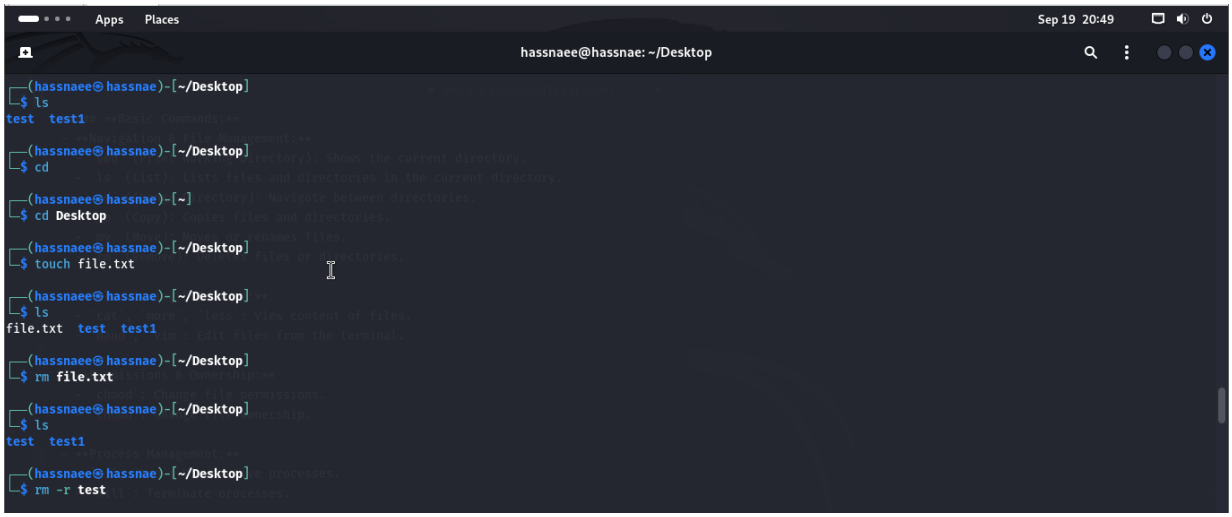

Home
KALI
Apps
Places
Sep 19 18:23
hassnaee@hassnae: ~
(hassnaee㉿hassnae)-[~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos 'sniffer (1).py' sniffer.py
(hassnaee㉿hassnae)-[~]
$ rm sniffer.py
(hassnaee㉿hassnae)-[~]
$ rm sniffer (1).py
rm: cannot remove 'sniffer': No such file or directory
rm: cannot remove '(1).py': No such file or directory
(hassnaee㉿hassnae)-[~]
$ rm 'sniffer (1).py'
(hassnaee㉿hassnae)-[~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
(hassnaee㉿hassnae)-[~]
$ cd Desktop
(hassnaee㉿hassnae)-[~/Desktop]
$ ls
(hassnaee㉿hassnae)-[~/Desktop]
$ cd ..

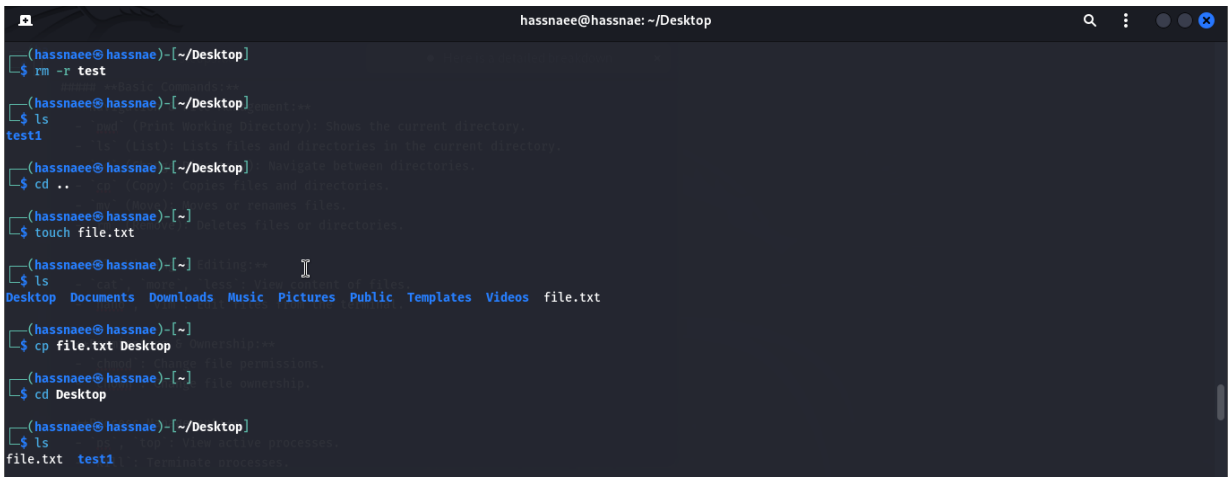

Apps
Places
Sep 19 18:57
hassnaee@hassnae: ~/Desktop/test
$ ls -la
total 144
drwx------ 16 hassnaee hassnaee 4096 Sep 19 18:21 .
drwxr-xr-x 3 root root 4096 Aug 18 17:18 ..
-rw-r--r-- 1 hassnaee hassnaee 220 Aug 18 17:18 .bash_logout
-rw-r--r-- 1 hassnaee hassnaee 5689 Aug 21 17:49 .bashrc
-rw-r--r-- 1 hassnaee hassnaee 3526 Aug 18 17:18 .bashrc.original
drwxrwxr-x 13 hassnaee hassnaee 4096 Aug 18 17:39 .cache
drwxr-xr-x 19 hassnaee hassnaee 4096 Sep 19 16:05 .config
-rw-r--r-- 1 hassnaee hassnaee 11759 Aug 18 17:18 .face
lrwxrwxrwx 1 hassnaee hassnaee 5 Aug 18 17:18 .face.icon -> .face
drwxr-xr-x 3 hassnaee hassnaee 4096 Aug 18 17:18 .java
drwxr-xr-x 4 hassnaee hassnaee 4096 Aug 18 17:21 .local
drwx------ 4 hassnaee hassnaee 4096 Aug 18 17:39 .mozilla
drwxrwxr-x 4 hassnaee hassnaee 4096 Aug 21 17:58 .npm
-rw-r--r-- 1 hassnaee hassnaee 807 Aug 18 17:18 .profile
-rw------- 1 hassnaee hassnaee 12288 Aug 18 18:26 .sniffer.py.swo
-rw-r--r-- 1 hassnaee hassnaee 0 Aug 18 17:25 .sudo_as_admin_successful
-rw------- 1 hassnaee hassnaee 7594 Aug 18 18:38 .viminfo
-rw-rw-r-- 1 hassnaee hassnaee 165 Aug 21 17:31 .wget-hsts
-rw------- 1 hassnaee hassnaee 9791 Sep 18 16:00 .zsh_history
-rw-r--r-- 1 hassnaee hassnaee 10868 Aug 18 17:18 .zshrc
drwxr-xr-x 2 hassnaee hassnaee 4096 Aug 18 17:21 Desktop
drwxr-xr-x 2 hassnaee hassnaee 4096 Aug 18 17:21 Documents
drwxr-xr-x 2 hassnaee hassnaee 4096 Sep 19 18:02 Downloads
drwxr-xr-x 2 hassnaee hassnaee 4096 Aug 18 17:21 Music
drwxr-xr-x 2 hassnaee hassnaee 4096 Aug 18 17:21 Pictures


Apps
Places
Sep 19 18:58
hassnaee@hassnae: ~/Desktop/test
drwxr-xr-x 2 hassnaee hassnaee 4096 Aug 18 17:21 Videos
(hassnaee㉿hassnae)-[~]
$ cd /dev
(hassnaee㉿hassnae)-[/dev]
$ ls
autofs cpu_dma_latency hpet loop2 net rtc snd tty12 tty21 tty30 tty4 tty49 tty58 ttyS0 vcs2 vcsa5 vga_arbiter
block cuse hugepages loop3 null rtc0 sr0 tty13 tty22 tty31 tty40 tty5 tty59 ttyS1 vcs3 vcsa6 vhci
bsg disk hwrng loop4 nvram sda stderr tty14 tty23 tty32 tty41 tty50 tty6 ttyS2 vcs4 vcsu vhost-net
btrfs-control dmmidi initctl loop5 port sda1 stdin tty15 tty24 tty33 tty42 tty51 tty60 ttyS3 vcs5 vcsu1 vhost-vsock
bus dri input loop6 ppp sda2 stdout tty16 tty25 tty34 tty43 tty52 tty61 uhid vcs6 vcsu2 vmci
cdrom fb0 kmsg loop7 psaux sda5 tty tty17 tty26 tty35 tty44 tty53 tty62 uinput vcsa vcsu3 vsock
char fd log mapper ptmx sg0 tty0 tty18 tty27 tty36 tty45 tty54 tty63 urandom vcsa1 vcsu4 zero
console full loop-control mem pts sg1 tty1 tty19 tty28 tty37 tty46 tty55 tty7 userfaultfd vcsa2 vcsu5
core fuse loop0 midi random shm tty10 tty2 tty29 tty38 tty47 tty56 tty8 vcs vcsa3 vcsu6
cpu hidraw0 loop1 mqueue rfkill snapshot tty11 tty20 tty3 tty39 tty48 tty57 tty9 vcs1 vcsa4 vfio
(hassnaee㉿hassnae)-[/dev]
$ cd ~/Desktop
(hassnaee㉿hassnae)-[~/Desktop]
$ cd ..
(hassnaee㉿hassnae)-[~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos


(hassnaee㉿hassnae)-[~]
$ rmdir test
(hassnaee㉿hassnae)-[~]
$ cd Desktop
(hassnaee㉿hassnae)-[~/Desktop]
$ mkdir test
(hassnaee㉿hassnae)-[~/Desktop]
$ ls
test


(hassnaee㉿hassnae)-[~/Desktop]
$ ls
test
(hassnaee㉿hassnae)-[~/Desktop]
$ mkdir -p test1/testsup
(hassnaee㉿hassnae)-[~/Desktop]
$ ls
test test1
(hassnaee㉿hassnae)-[~/Desktop]
$ cd test 1
cd: string not in pwd: test
(hassnaee㉿hassnae)-[~/Desktop]
$ cd test1
(hassnaee㉿hassnae)-[~/Desktop/test1]
$ ls
testsup
(hassnaee㉿hassnae)-[~/Desktop/test1]
$ cd
(hassnaee㉿hassnae)-[~]
$ cd Desktop


Apps Places
Sep 19 20:49
hassnaee@hassnae: ~/Desktop
(hassnaee㉿hassnae)-[~/Desktop]
$ ls
test test1
(hassnaee㉿hassnae)-[~/Desktop]
$ cd
(hassnaee㉿hassnae)-[~]
$ cd Desktop
(hassnaee㉿hassnae)-[~/Desktop]
$ touch file.txt
(hassnaee㉿hassnae)-[~/Desktop]
$ ls
file.txt test test1
(hassnaee㉿hassnae)-[~/Desktop]
$ rm file.txt
(hassnaee㉿hassnae)-[~/Desktop]
$ ls
test test1
(hassnaee㉿hassnae)-[~/Desktop]
$ rm -r test


hassnaee@hassnae: ~/Desktop
(hassnaee㉿hassnae)-[~/Desktop]
$ rm -r test
(hassnaee㉿hassnae)-[~/Desktop]
$ ls
test1
(hassnaee㉿hassnae)-[~/Desktop]
$ cd ..
(hassnaee㉿hassnae)-[~]
$ touch file.txt
(hassnaee㉿hassnae)-[~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos file.txt
(hassnaee㉿hassnae)-[~]
$ cp file.txt Desktop
(hassnaee㉿hassnae)-[~]
$ cd Desktop
(hassnaee㉿hassnae)-[~/Desktop]
$ ls
file.txt test1

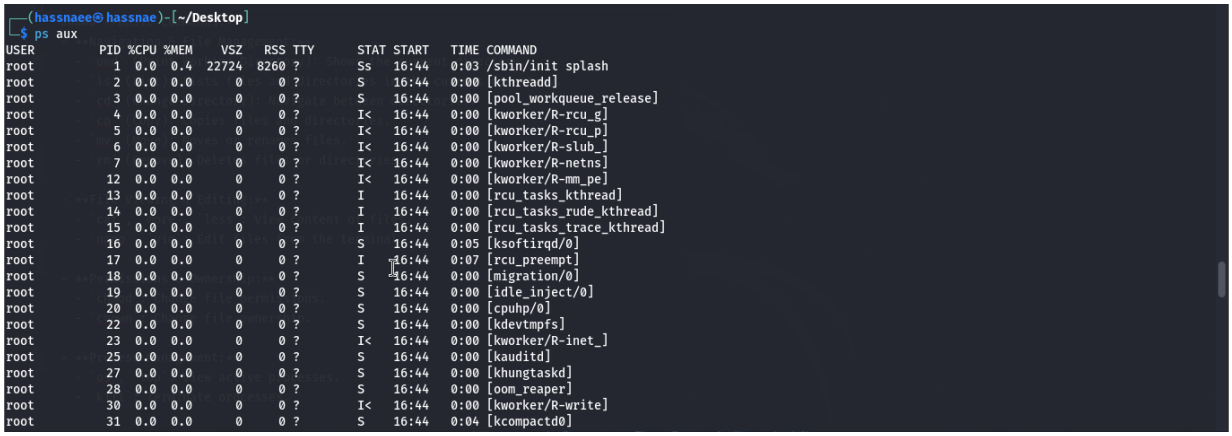
```
┌──(hassnaee㉿hassnae)-[~/Desktop]
└─$ nano file.txt

┌──(hassnaee㉿hassnae)-[~/Desktop]
└─$ cat file.txt
Hi !
My name is hassne elkabir
```

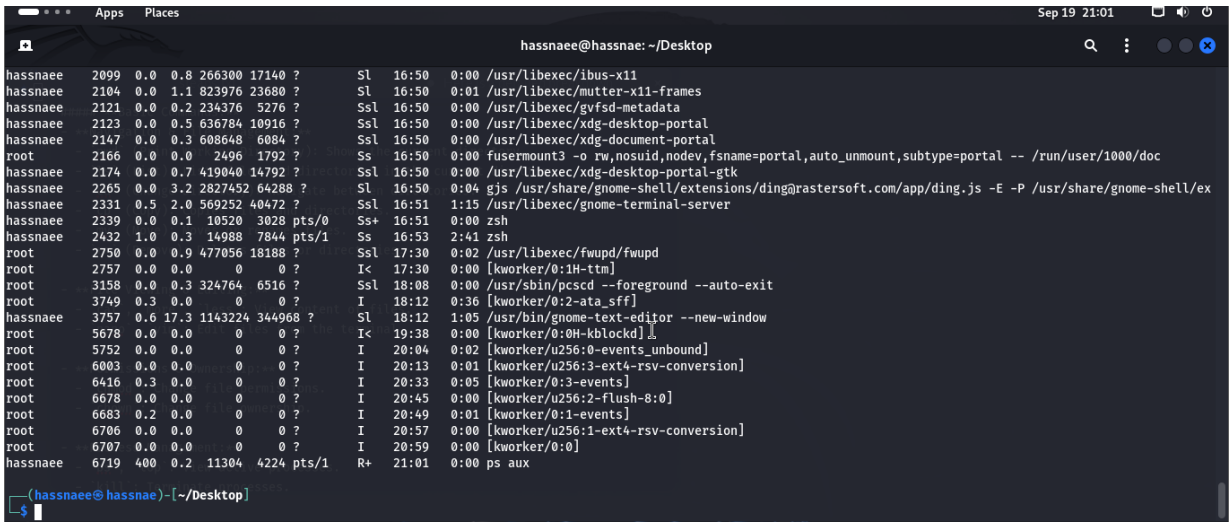
```
Apps  Places                                                    Sep 19 20:18
hassnaee@hassnae: ~/Desktop
 GNU nano 8.0                                  file.txt *
Hi !
My name is hassne elkabir
```

```
hassnaee@hassnae: ~/Desktop
┌──(hassnaee㉿hassnae)-[~/Desktop]
└─$ touch newfile.txt

┌──(hassnaee㉿hassnae)-[~/Desktop]
└─$ ls
file.txt  newfile.txt  test1

┌──(hassnaee㉿hassnae)-[~/Desktop]
└─$ cat newfile.txt

┌──(hassnaee㉿hassnae)-[~/Desktop]
└─$ nano newfile.txt

┌──(hassnaee㉿hassnae)-[~/Desktop]
└─$ cat newfile.txt
Hello again

┌──(hassnaee㉿hassnae)-[~/Desktop]
└─$ touch script.sh

┌──(hassnaee㉿hassnae)-[~/Desktop]
└─$ nano script.sh
```

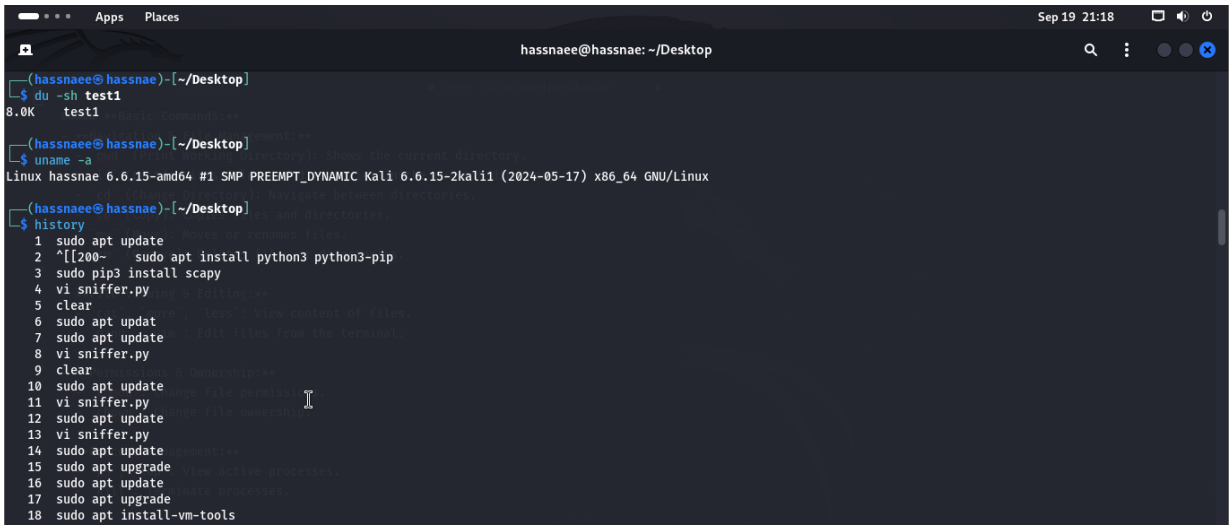
```
Apps  Places                                                    Sep 19 20:54
hassnaee@hassnae: ~/Desktop
 GNU nano 8.0                                  script.sh
#!/bin/bash
mkdir NewFolder
cd NewFolder
ls

                              [ Read 4 lines ]
^G Help        ^O Write Out   ^F Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark     M-] To Bracket  M-B Previous
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6 Copy         ^B Where Was    M-F Next
```


(hassnaee㉿hassnae)-[~/Desktop]
$ nano script.sh
(hassnaee㉿hassnae)-[~/Desktop]
$ cat script.sh
# /bin/bash
mkdir NewFolder
cd NewFolder
ls
(hassnaee㉿hassnae)-[~/Desktop]
$ ./script.sh
zsh: permission denied: ./script.sh
(hassnaee㉿hassnae)-[~/Desktop]
$ chmod u+x script.sh
(hassnaee㉿hassnae)-[~/Desktop]
$ ./script.sh
(hassnaee㉿hassnae)-[~/Desktop]
$ ls
NewFolder file.txt newfile.txt script.sh test1
(hassnaee㉿hassnae)-[~/Desktop]
$ echo 'System and Process Management'
System and Process Management

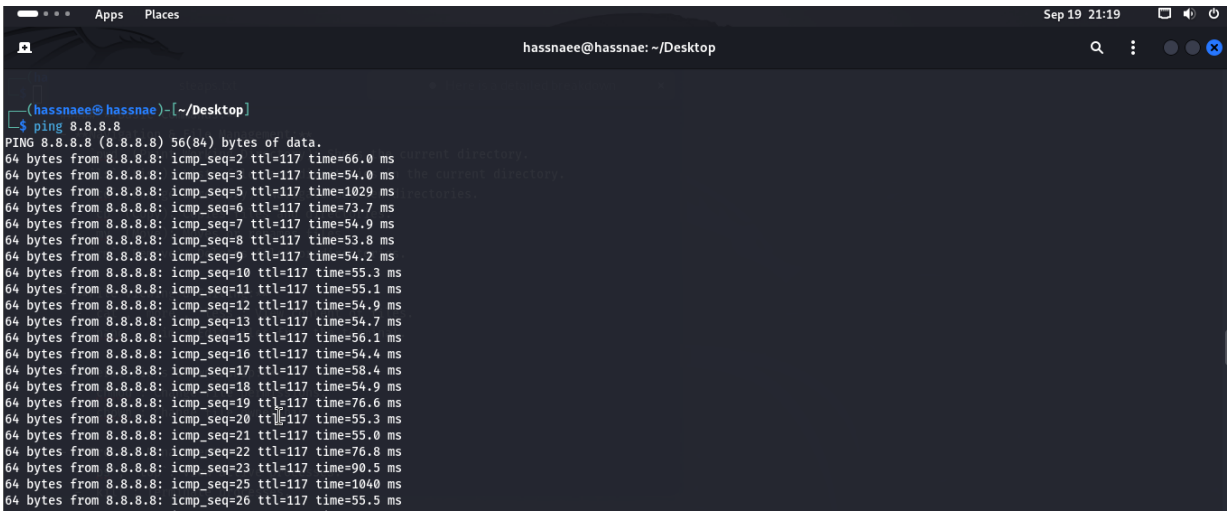

(hassnaee㉿hassnae)-[~/Desktop]
$ ps aux
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 0.0 0.4 22724 8260 ? Ss 16:44 0:03 /sbin/init splash
root 2 0.0 0.0 0 0 ? S 16:44 0:00 [kthreadd]
root 3 0.0 0.0 0 0 ? S 16:44 0:00 [pool_workqueue_release]
root 4 0.0 0.0 0 0 ? I< 16:44 0:00 [kworker/R-rcu_g]
root 5 0.0 0.0 0 0 ? I< 16:44 0:00 [kworker/R-rcu_p]
root 6 0.0 0.0 0 0 ? I< 16:44 0:00 [kworker/R-slub_]
root 7 0.0 0.0 0 0 ? I< 16:44 0:00 [kworker/R-netns]
root 12 0.0 0.0 0 0 ? I< 16:44 0:00 [kworker/R-mm_pe]
root 13 0.0 0.0 0 0 ? I 16:44 0:00 [rcu_tasks_kthread]
root 14 0.0 0.0 0 0 ? I 16:44 0:00 [rcu_tasks_rude_kthread]
root 15 0.0 0.0 0 0 ? I 16:44 0:00 [rcu_tasks_trace_kthread]
root 16 0.0 0.0 0 0 ? S 16:44 0:05 [ksoftirqd/0]
root 17 0.0 0.0 0 0 ? I 16:44 0:07 [rcu_preempt]
root 18 0.0 0.0 0 0 ? S 16:44 0:00 [migration/0]
root 19 0.0 0.0 0 0 ? S 16:44 0:00 [idle_inject/0]
root 20 0.0 0.0 0 0 ? S 16:44 0:00 [cpuhp/0]
root 22 0.0 0.0 0 0 ? S 16:44 0:00 [kdevtmpfs]
root 23 0.0 0.0 0 0 ? I< 16:44 0:00 [kworker/R-inet_]
root 25 0.0 0.0 0 0 ? S 16:44 0:00 [kauditd]
root 27 0.0 0.0 0 0 ? S 16:44 0:00 [khungtaskd]
root 28 0.0 0.0 0 0 ? S 16:44 0:00 [oom_reaper]
root 30 0.0 0.0 0 0 ? I< 16:44 0:00 [kworker/R-write]
root 31 0.0 0.0 0 0 ? S 16:44 0:04 [kcompactd0]

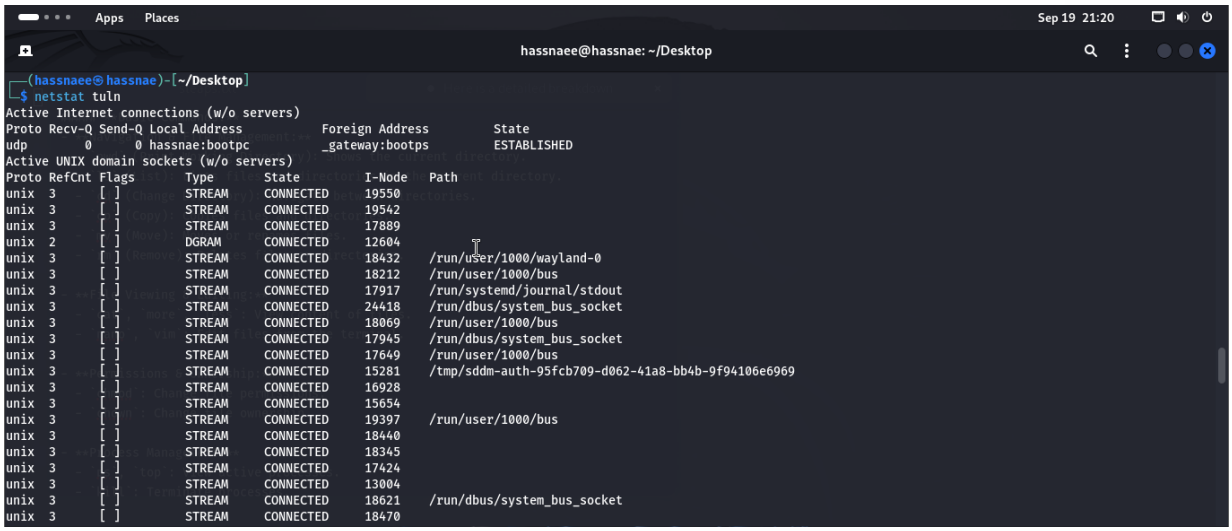

Apps Places
Sep 19 21:01
hassnaee@hassnae: ~/Desktop
hassnaee 2099 0.0 0.8 266300 17140 ? Sl 16:50 0:00 /usr/libexec/ibus-x11
hassnaee 2104 0.0 1.1 823976 23680 ? Sl 16:50 0:01 /usr/libexec/mutter-x11-frames
hassnaee 2121 0.0 0.2 234376 5276 ? Ssl 16:50 0:00 /usr/libexec/gvfsd-metadata
hassnaee 2123 0.0 0.5 636784 10916 ? Ssl 16:50 0:00 /usr/libexec/xdg-desktop-portal
hassnaee 2147 0.0 0.3 608648 6084 ? Ssl 16:50 0:00 /usr/libexec/xdg-document-portal
root 2166 0.0 0.0 2496 1792 ? Ss 16:50 0:00 fusermount3 -o rw,nosuid,nodev,fsname=portal,auto_unmount,subtype=portal -- /run/user/1000/doc
hassnaee 2174 0.0 0.7 419040 14792 ? Ssl 16:50 0:00 /usr/libexec/xdg-desktop-portal-gtk
hassnaee 2265 0.0 3.2 2827452 64288 ? Sl 16:50 0:04 gjs /usr/share/gnome-shell/extensions/ding@rastersoft.com/app/ding.js -E -P /usr/share/gnome-shell/ex
hassnaee 2331 0.5 2.0 569252 40472 ? Ssl 16:51 1:15 /usr/libexec/gnome-terminal-server
hassnaee 2339 0.0 0.1 10520 3028 pts/0 Ss+ 16:51 0:00 zsh
hassnaee 2432 1.0 0.3 14988 7844 pts/1 Ss 16:53 2:41 zsh
root 2750 0.0 0.9 477056 18188 ? Ssl 17:30 0:02 /usr/libexec/fwupd/fwupd
root 2757 0.0 0.0 0 0 ? I< 17:30 0:00 [kworker/0:1H-ttm]
root 3158 0.0 0.3 324764 6516 ? Ssl 18:08 0:00 /usr/sbin/pcscd --foreground --auto-exit
root 3749 0.3 0.0 0 0 ? I 18:12 0:36 [kworker/0:2-ata_sff]
hassnaee 3757 0.6 17.3 1143224 344968 ? Sl 18:12 1:05 /usr/bin/gnome-text-editor --new-window
root 5678 0.0 0.0 0 0 ? I< 19:38 0:00 [kworker/0:0H-kblockd]
root 5752 0.0 0.0 0 0 ? I 20:04 0:02 [kworker/u256:0-events_unbound]
root 6003 0.0 0.0 0 0 ? I 20:13 0:01 [kworker/u256:3-ext4-rsv-conversion]
root 6416 0.3 0.0 0 0 ? I 20:33 0:05 [kworker/0:3-events]
root 6678 0.0 0.0 0 0 ? I 20:45 0:00 [kworker/u256:2-flush-8:0]
root 6683 0.2 0.0 0 0 ? I 20:49 0:01 [kworker/0:1-events]
root 6706 0.0 0.0 0 0 ? I 20:57 0:00 [kworker/u256:1-ext4-rsv-conversion]
root 6707 0.0 0.0 0 0 ? I 20:59 0:00 [kworker/0:0]
hassnaee 6719 400 0.2 11304 4224 pts/1 R+ 21:01 0:00 ps aux
(hassnaee㉿hassnae)-[~/Desktop]
$

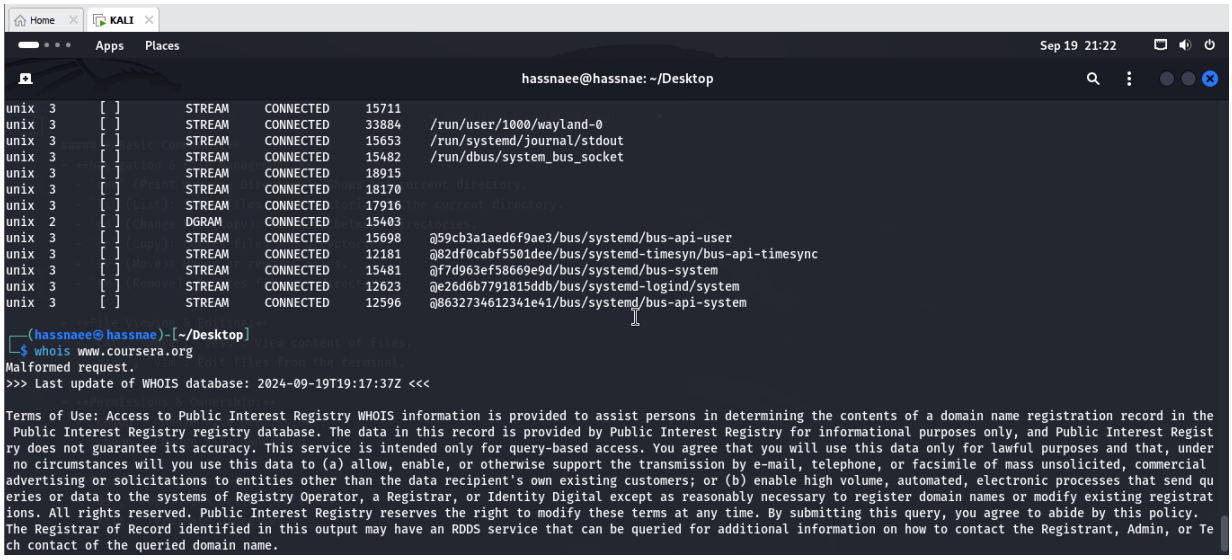

Apps Places
Sep 19 21:18
hassnaee@hassnae: ~/Desktop
(hassnaee㉿hassnae)-[~/Desktop]
$ df -h
Filesystem Size Used Avail Use% Mounted on
udev 929M 0 929M 0% /dev
tmpfs 195M 1.5M 193M 1% /run
/dev/sda1 19G 17G 963M 95% /
tmpfs 971M 0 971M 0% /dev/shm
tmpfs 5.0M 0 5.0M 0% /run/lock
tmpfs 195M 192K 194M 1% /run/user/1000


Apps Places
Sep 19 21:18
hassnaee@hassnae: ~/Desktop
(hassnaee㉿hassnae)-[~/Desktop]
$ du -sh test1
8.0K test1
(hassnaee㉿hassnae)-[~/Desktop]
$ uname -a
Linux hassnae 6.6.15-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.15-2kali1 (2024-05-17) x86_64 GNU/Linux
(hassnaee㉿hassnae)-[~/Desktop]
$ history
1 sudo apt update
2 ^[[200~ sudo apt install python3 python3-pip
3 sudo pip3 install scapy
4 vi sniffer.py
5 clear
6 sudo apt updat
7 sudo apt update
8 vi sniffer.py
9 clear
10 sudo apt update
11 vi sniffer.py
12 sudo apt update
13 vi sniffer.py
14 sudo apt update
15 sudo apt upgrade
16 sudo apt update
17 sudo apt upgrade
18 sudo apt install-vm-tools


501 top
502 ps aux
503 df -h
504 df -sh
505 df -Sh
506 du -sh test1
507 uname -a
(hassnaee㉿hassnae)-[~/Desktop]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.1.107 netmask 255.255.255.0 broadcast 192.168.1.255
inet6 fe80::20c:29ff:fe56:6a7f prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:56:6a:7f txqueuelen 1000 (Ethernet)
RX packets 74967 bytes 97970648 (93.4 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 29881 bytes 2466976 (2.3 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 28 bytes 1680 (1.6 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 28 bytes 1680 (1.6 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0


Apps Places
Sep 19 21:19
hassnaee@hassnae: ~/Desktop
(hassnaee㉿hassnae)-[~/Desktop]
$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=66.0 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=54.0 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=117 time=1029 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=117 time=73.7 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=117 time=54.9 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=117 time=53.8 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=117 time=54.2 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=117 time=55.3 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=117 time=55.1 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=117 time=54.9 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=117 time=54.7 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=117 time=56.1 ms
64 bytes from 8.8.8.8: icmp_seq=16 ttl=117 time=54.4 ms
64 bytes from 8.8.8.8: icmp_seq=17 ttl=117 time=58.4 ms
64 bytes from 8.8.8.8: icmp_seq=18 ttl=117 time=54.9 ms
64 bytes from 8.8.8.8: icmp_seq=19 ttl=117 time=76.6 ms
64 bytes from 8.8.8.8: icmp_seq=20 ttl=117 time=55.3 ms
64 bytes from 8.8.8.8: icmp_seq=21 ttl=117 time=55.0 ms
64 bytes from 8.8.8.8: icmp_seq=22 ttl=117 time=76.8 ms
64 bytes from 8.8.8.8: icmp_seq=23 ttl=117 time=90.5 ms
64 bytes from 8.8.8.8: icmp_seq=25 ttl=117 time=1040 ms
64 bytes from 8.8.8.8: icmp_seq=26 ttl=117 time=55.5 ms





3. Install Kali Linux Tools from GitHub:

We can install various hacking tools from GitHub on Kali Linux. Here's how you can do it :

- Search for a tool on GitHub, for example, a network scanner or password cracker.

Let's use nmap (network scanning tool) as an example:

Steps:

Clone the repository:
In this example, SQLmap was cloned using this command:

```
git clone --depth 1 https://github.com/sqlmapproject/sqlmap.git
```

This downloaded the SQLmap tool onto the desktop.
Navigate to the tool directory:
Use the cd command to move to the directory:

```
cd sqlmap
```

Run the tool:
To run SQLmap, we need to execute the following:

```
python sqlmap.py
```

Perform a test scan:
Test with a vulnerable URL:

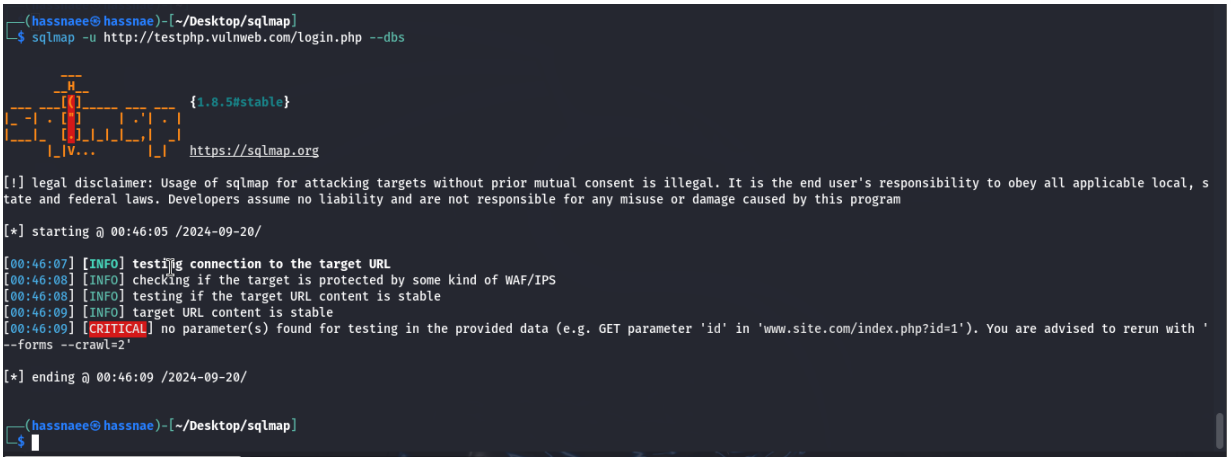
```
sqlmap -u http://testphp.vulnweb.com/login.php --dbs
```

This will initiate SQLmap to scan for databases on the target site.

```
┌──(hassnaee㉿hassnae)-[~/Desktop]
└─$ echo "install tools from github"
install tools from github
```

```
┌──(hassnaee㉿hassnae)-[~/Desktop]
└─$ git clone --depth 1 https://github.com/sqlmapproject/sqlmap.git
Cloning into 'sqlmap'...
remote: Enumerating objects: 733, done.
remote: Counting objects: 100% (733/733), done.
remote: Compressing objects: 100% (489/489), done.
remote: Total 733 (delta 249), reused 505 (delta 231), pack-reused 0 (from 0)
Receiving objects: 100% (733/733), 7.01 MiB | 158.00 KiB/s, done.
Resolving deltas: 100% (249/249), done.
Updating files: 100% (640/640), done.

┌──(hassnaee㉿hassnae)-[~/Desktop]
└─$ ls
NewFolder  file.txt  newfile.txt  script.sh  sqlmap  sqlmap-dev  test1
```

```
┌──(hassnaee㉿hassnae)-[~/Desktop]
└─$ ls
NewFolder  file.txt  newfile.txt  script.sh  sqlmap  sqlmap-dev  test1

┌──(hassnaee㉿hassnae)-[~/Desktop]
└─$ cd sqlmap

┌──(hassnaee㉿hassnae)-[~/Desktop/sqlmap]
└─$ ls
LICENSE  README.md  data  doc  extra  lib  plugins  sqlmap.conf  sqlmap.py  sqlmapapi.py  sqlmapapi.yaml  tamper  thirdparty

┌──(hassnaee㉿hassnae)-[~/Desktop/sqlmap]
└─$ python sqlmap.py
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.8.9#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

Usage: python sqlmap.py [options]

sqlmap.py: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c, --wizard, --shell, --update, --purge, --list-tampers or --dependencies). Use -h for basic and
-hh for advanced help
```


┌──(hassnaee㉿hassnae)-[~/Desktop/sqlmap]
└─$ sqlmap -u http://testphp.vulnweb.com/login.php --dbs
{1.8.5#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 00:46:05 /2024-09-20/
[00:46:07] [INFO] testing connection to the target URL
[00:46:08] [INFO] checking if the target is protected by some kind of WAF/IPS
[00:46:08] [INFO] testing if the target URL content is stable
[00:46:09] [INFO] target URL content is stable
[00:46:09] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1'). You are advised to rerun with '--forms --crawl=2'
[*] ending @ 00:46:09 /2024-09-20/
┌──(hassnaee㉿hassnae)-[~/Desktop/sqlmap]
└─$