Department\Cyber Security
Group\ Second
Assignment\ Second
Eng. Alshebli Fisal Ahmeb Al-Shebli

بســـم الرحيـــم الله الرحمـــن

الجمهورية اليمنية
وزارة التعليم العالي والبحث العلمي
جامعـــــة الـــــــــرازي
كلية الحاسوب وتقنية المعلومات

SOME KALI LINUX COMMANDS

SECTION 1: FILE AND DIRECTORY MANAGEMENT

1. **Display the current working directory.**

يعرض المسار الكامل للمجلد الحالي الذي تعمل فيه. يُستخدم لمعرفة موقعك داخل نظام الملفات.

```
┌──(kali㉿kali)-[~]
└─$ pwe
Command 'pwe' not found, did you mean:
  command 'wpe' from deb xwpe
  command 'we' from deb xwpe
  command 'pwm' from deb python3-passwordmeter
  command 'xwe' from deb xwpe
  command 'pee' from deb moreutils
  command 'pwd' from deb coreutils
Try: sudo apt install <deb name>

┌──(kali㉿kali)-[~]
└─$
```

2. **List all the contents of your current directory, including hidden files.**

يعرض جميع الملفات والمجلدات في الدليل الحالي، بما في ذلك الملفات المخفية. يساعد في معرفة محتويات المجلد.

```
┌──(kali㉿kali)-[~]
└─$ ls -a
.                   Downloads        Pictures
..                  estfile.txt      .profile
backup_testfile.txt .face            Public
.bash_logout        .face.icon       .sudo_as_admin_successful
.bashrc             .gnupg           Templates
.bashrc.original    .ICEauthority    Videos
.cache              .java            .Xauthority
.config             .local           .xsession-errors
Desktop             .mozilla         .xsession-errors.old
.dmrc               Music            .zsh_history
Documents           newfile.txt      .zshrc
```

3. **Change your directory to the `Desktop`.**

يُستخدم لتغيير الدليل الحالي إلى دليل آخر. في هذا المثال، ينتقل إلى مجلد سطح المكتب.

```
┌──(kali㉿kali)-[~]
└─$ cd ~/Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$
```

4. **Create two directories named `dir1` and `dir2` on the Desktop.**

يُستخدم لإنشاء مجلدات جديدة. في هذا المثال، ينشئ مجلدين باسم `dir1` و `dir2`.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ mkdir dir1 dir2

┌──(kali㉿kali)-[~/Desktop]
└─$
```

5. **Inside `dir1`, create a file named `file1.txt`.**

يُستخدم لإنشاء ملفات فارغة جديدة. هنا، ينشئ ملفات نصية فارغة داخل مجلدات معينة.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ mkdir dir1 dir2

┌──(kali㉿kali)-[~/Desktop]
└─$ touch ~/Desktop/dir1/alshbli1.txt
```

6. **Inside `dir2`, create a file named `file2.txt`.**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ touch ~/Desktop/dir2/alshbli2.txt
```

7. **Using nano or vim Write the numbers 1 to 9 into `file1.txt`.**

محررات نصوص تُستخدم لتحرير الملفات النصية من خلال واجهة سطر الأوامر.

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ nano ~/Desktop/dir2/alshbli2.txt
```

8. **From the home directory Copy the contents of `file1.txt` into `file2.txt`.**

يُستخدم لنسخ الملفات أو المجلدات من موقع إلى آخر. هنا، ينقل محتويات ملف إلى ملف آخر.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cp /home/kali/Desktop/dir1/alshbli1.txt /home/kali/Desktop/dir2/alshbli2.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ cat dir2/alshbli2.txt
1
2
3
4
5
6
7
8
9
```

9. **From the home directory, delete `file1.txt` inside `dir1`.**

يُستخدم لحذف الملفات. في هذا المثال، يقوم بحذف ملف معين.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ rm dir1/alshbli1.txt

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
dir1  dir2  quiz02.sh

┌──(kali㉿kali)-[~/Desktop]
└─$ cd dir1

┌──(kali㉿kali)-[~/Desktop/dir1]
└─$ ls

┌──(kali㉿kali)-[~/Desktop/dir1]
└─$
```

10. **Remove the directory `dir1` from the Desktop.**

يُستخدم لحذف مجلد فارغ.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ rmdir dir1

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
dir2  quiz02.sh
```

11. **Redirect the output of the network configuration command to a file named `network_info.txt` on the Desktop.**

يقوم بتوجيه مخرجات أمر `ifconfig` إلى ملف بدلاً من عرضها على الشاشة. يُستخدم لحفظ معلومات الشبكة في ملف.

```
┌──(kali㉿kali)-[~]
└─$ ifconfing > ~/Desktop/network_info.txt
Command 'ifconfing' not found, did you mean:
  command 'ifconfig' from deb net-tools
Try: sudo apt install <deb name>
```

12. **Open the Desktop folder and show all files with detailed information.**

يُستخدم لعرض ملفات المجلد الحالي مع جميع التفاصيل مثل الأذونات، المالك، وحجم الملف.

```
┌──(kali㉿kali)-[~]
└─$ ls -l
total 32
-rw-r--r-- 1 kali kali    0 Aug  3 12:36 backup_testfile.txt
drwxr-xr-x 3 kali kali 4096 Sep  3 13:49 Desktop
drwxr-xr-x 2 kali kali 4096 Jul 15 11:05 Documents
drwxr-xr-x 2 kali kali 4096 Jul 15 11:05 Downloads
-rw-r--r-- 1 kali kali    0 Aug  3 12:33 estfile.txt
drwxr-xr-x 2 kali kali 4096 Jul 15 11:05 Music
-rw-r--r-- 1 kali kali    0 Aug  3 12:36 newfile.txt
drwxr-xr-x 2 kali kali 4096 Jul 15 11:05 Pictures
drwxr-xr-x 2 kali kali 4096 Jul 15 11:05 Public
drwxr-xr-x 2 kali kali 4096 Jul 15 11:05 Templates
drwxr-xr-x 2 kali kali 4096 Jul 15 11:05 Videos
```

SECTION 2: USERS AND GROUPS MANAGEMENT

13. **Create a new user with your name.**

يُستخدم لإنشاء حساب مستخدم جديد على النظام.

```
┌──(kali㉿kali)-[~]
└─$ sudo adduser alshebli_2003
info: Adding user `alshebli_2003' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `alshebli_2003' (1003) ...
info: Adding new user `alshebli_2003' (1003) with group `alshebli_2003 (1003)' ...
info: Creating home directory `/home/alshebli_2003' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for alshebli_2003
Enter the new value, or press ENTER for the default
        Full Name []: alshebli faisal
        Room Number []: 2000
        Work Phone []: 770626671
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `alshebli_2003' to supplemental / extra groups `users' ...
info: Adding user `alshebli_2003' to group `users' ...
```

14. **Set a password for your user.**

يُستخدم لتعيين أو تغيير كلمة المرور للمستخدم.

```
┌──(kali㉿kali)-[~]
└─$ sudo passwd alshebli_2003
New password:
Retype new password:
passwd: password updated successfully
```

15. **Open the file that contains user information and verify that your user has been added.**

يعرض محتويات ملف `passwd` الذي يحتوي على معلومات المستخدمين في النظام.

```
┌──(kali㉿kali)-[~]
└─$ cat /etc/passwd | grep alshebli_2003
alshebli_2003:x:1003:1003:alshebli faisal,2000,770626671,:/home/alshebli_2003:/bin/bash

┌──(kali㉿kali)-[~]
└─$
```

16. **Add your user to the file that gives administrative privileges.**

يُستخدم لإضافة مستخدم إلى مجموعة معينة.

```
┌──(kali㉿kali)-[~]
└─$ sudo usermod -aG sudo alshebl_2003
[sudo] password for kali:
usermod: user 'alshebl_2003' does not exist

┌──(kali㉿kali)-[~]
└─$ sudo usermod -aG sudo alshebli_2003

┌──(kali㉿kali)-[~]
└─$ groups alshebli_2003
alshebli_2003 : alshebli_2003 sudo users

┌──(kali㉿kali)-[~]
└─$ su - alshebli_2003
Password:
┌──(alshebli_2003㉿kali)-[~]
└─$ sudo ls /root
[sudo] password for alshebli_2003:
```

17. **Switch to your user and confirm the user identity.**

يُستخدم لتبديل المستخدم النشط إلى مستخدم آخر.

```
┌──(alshebli_2003㉿kali)-[~]
└─$ su alshebli_2003 whoami
Password:
/usr/bin/whoami: /usr/bin/whoami: cannot execute binary file

┌──(alshebli_2003㉿kali)-[~]
└─$
```

18. **Create a new group named `testgroup`.**

يُستخدم لإنشاء مجموعة جديدة.

```
┌──(alshebli_2003㉿kali)-[~]
└─$ sudo groupadd testgroup
[sudo] password for alshebli_2003:
```

19. **Add your user to `testgroup`.**

إضافة المستخدم الخاص بي الى **" testgroup"**

```
┌──(alshebli_2003㉿kali)-[~]
└─$ sudo usermod -aG testgroup alshebli_2003

┌──(alshebli_2003㉿kali)-[~]
└─$ id alshebli_2003
uid=1003(alshebli_2003) gid=1003(alshebli_2003) groups=1003(alshebli_2003),27(sudo),100(users),1004(testgroup)
```

20. **Add the group `testgroup` to the file that gives administrative privileges.**

إضافة `testgroup` إلى ملف يعطي صلاحيات إدارية:

```
┌──(kali㉿kali)-[~]
└─$ sudo usermod -aG sudo  testgroup alshebli_2003
Usage: usermod [options] LOGIN

Options:
  -a, --append                  append the user to the supplemental GROUPS
                                mentioned by the -G option without removing
                                the user from other groups
  -b, --badname                 allow bad names
  -c, --comment COMMENT         new value of the GECOS field
  -d, --home HOME_DIR           new home directory for the user account
  -e, --expiredate EXPIRE_DATE  set account expiration date to EXPIRE_DATE
  -f, --inactive INACTIVE       set password inactive after expiration
                                to INACTIVE
  -g, --gid GROUP               force use GROUP as new primary group
  -G, --groups GROUPS           new list of supplementary GROUPS
  -h, --help                    display this help message and exit
  -l, --login NEW_LOGIN         new value of the login name
  -L, --lock                    lock the user account
  -m, --move-home               move contents of the home directory to the
                                new location (use only with -d)
  -o, --non-unique              allow using duplicate (non-unique) UID
  -p, --password PASSWORD       use encrypted password for the new password
  -P, --prefix PREFIX_DIR       prefix directory where are located the /etc/* files
  -r, --remove                  remove the user from only the supplemental GROUPS
                                mentioned by the -G option without removing
                                the user from other groups
  -R, --root CHROOT_DIR         directory to chroot into
  -s, --shell SHELL             new login shell for the user account
  -u, --uid UID                 new UID for the user account
  -U, --unlock                  unlock the user account
  -v, --add-subuids FIRST-LAST  add range of subordinate uids
  -V, --del-subuids FIRST-LAST  remove range of subordinate uids
  -w, --add-subgids FIRST-LAST  add range of subordinate gids
  -W, --del-subgids FIRST-LAST  remove range of subordinate gids
  -Z, --selinux-user SEUSER     new SELinux user mapping for the user account
```

21. **Remove your user from the file that gives administrative privileges.**

إزالة المستخدم الخاص بك من الملف الذي يعطيه صلاحيات إدارية:

```
┌──(kali㉿kali)-[~]
└─$ sudo deluser alshebli_2003 sudo
info: Removing user `alshebli_2003' from group `sudo' ...
```

22. **Check if your user still have administrative privileges.**

التحقق مما إذا كان المستخدم لا يزال لديه صلاحيات إدارية:

```
┌──(kali㉿kali)-[~]
└─$ sudo -l
Matching Defaults entries for kali on kali:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User kali may run the following commands on kali:
    (ALL : ALL) ALL

┌──(kali㉿kali)-[~]
└─$ sudo -l /root
sudo: /root: command not found

┌──(kali㉿kali)-[~]
└─$
```

23. **Check which groups your user belongs to.**

التحقق من المجموعات التي ينتمي إليها المستخدم:

```
┌──(kali㉿kali)-[~]
└─$ groups alshebli_2003
alshebli_2003 : alshebli_2003 users testgroup
```

SECTION 3: PERMISSIONS AND OWNERSHIP

24. **Set the permissions of `file2.txt` on the Desktop to allow the owner to read, write, and execute; the group to read and execute; and others to read .**

تعيين صلاحيات الملف `alshbli2.txt` على سطح المكتب:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ chmod 775 dir2/alshbli2.txt
```

25. **Check the permissions of `file2.txt` to verify the change.**

التحقق من صلاحيات `alshbli2.txt`:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls -l dir2/alshbli2.txt
-rwxrwxr-x 1 kali kali 18 Sep  3 13:14 dir2/alshbli2.txt
```

26. **Change the ownership of `file2.txt` to your user**

تغيير ملكية `alshbli2.txt` إلى المستخدم الخاص بك

```
┌──(kali㉿kali)-[~]
└─$ sudo chown alshebli_2003 ~/Desktop/dir2/alshbli2.txt
[sudo] password for kali:
```

27. **verify the ownership of `file2.txt`.**

التحقق من ملكية `alshbli2.txt`:

```
┌──(kali㉿kali)-[~]
└─$ ls -l ~/Desktop/dir2/alshbli2.txt
-rwxrwxr-x 1 alshebli_2003 kali 18 Sep  3 13:14 /home/kali/Desktop/dir2/alshbli2.txt
```

28. **Change back the ownership of a file `file2.txt` .**

إعادة تغيير ملكية `alshbli2.txt`:

```
┌──(kali㉿kali)-[~]
└─$ sudo chown root  ~/Desktop/dir2/alshbli2.txt
[sudo] password for kali:
```

29. **Grant write permission to everyone for `file2.txt`.**

منح الجميع صلاحية الكتابة على `alshbli2.txt`:

```
┌──(kali㉿kali)-[~]
└─$ sudo chmod a+w ~/Desktop/dir2/alshbli2.txt

┌──(kali㉿kali)-[~]
└─$ ls -l ~/Desktop/dir2/alshbli2.txt
-rwxrwxrwx 1 root kali 18 Sep  3 13:14 /home/kali/Desktop/dir2/alshbli2.txt
```

30. **Remove the write permission for the group and others for `file2.txt`.**

إزالة صلاحية الكتابة للمجموعة والآخرين:

```
┌──(kali㉿kali)-[~]
└─$ sudo chmod go-w ~/Desktop/dir2/alshbli2.txt

┌──(kali㉿kali)-[~]
└─$ ls -l ~/Desktop/dir2/alshbli2.txt
-rwxr-xr-x 1 root kali 18 Sep  3 13:14 /home/kali/Desktop/dir2/alshbli2.txt
```

31. **Delete `file2.txt` after making the necessary ownership and permission changes.**

حذف `alshbli2.txt` بعد تغيير الملكية والصلاحيات الضرورية:

```
┌──(kali㉿kali)-[~]
└─$ sudo rm ~/Desktop/dir2/alshbli2.txt

┌──(kali㉿kali)-[~]
└─$ ls -l ~/Desktop/dir2
total 0
```

32. **What command would you use to recursively change the permissions of all files and directories inside a folder named `Desktop` to `755`.**

تغيير الصلاحيات لجميع الملفات والمجلدات داخل مجلد `Desktop` إلى `755` بشكل تكراري:

```
┌──(kali㉿kali)-[~]
└─$ chmod -R 755 ~/Desktop
```

SECTION 4: PROCESS MANAGEMENT

33. **Install a system monitor tool that provides an interactive process viewer(htop).**

تثبيت أداة مراقبة العمليات `htop`:

```
┌──(sir㉿kali)-[~]
└─$ sudo apt install htop
htop is already the newest version (3.3.0-4).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 425
```

34. **Display all running processes.**

عرض جميع العمليات الجارية:

There are many ways to display all running processes:

- ps aux
- top
- htop
- pgrep -a
- pstree

```
  0[||                          1.9%] Tasks: 84, 198 thr, 78 kthr; 1 running
  1[|||                         7.0%] Load average: 0.37 0.24 0.14
  2[|                           0.6%] Uptime: 01:06:54
Mem[||||||||||            666M/5.80G]
Swp[                        0K/976M]

 Main   I/O
   PID USER      PRI  NI  VIRT   RES   SHR S  CPU%▽MEM%   TIME+  Command
 33605 sir        20   0  8580  4352  3200 R   3.2  0.1  0:00.19 htop
   863 root       20   0  428M   126M 56432 S   2.6  2.1  0:40.07 /usr/lib/xorg/Xorg
  1129 sir        20   0  210M  3204  2944 S   0.6  0.1  0:00.46 /usr/bin/VBoxClien
  1164 sir        20   0  579M 93824 73592 S   0.6  1.5  0:14.52 xfwm4 --display :0
  1221 sir        20   0  289M 56552 19328 S   0.6  0.9  0:11.90 /usr/lib/x86_64-li
  1223 sir        20   0  332M 29864 20724 S   0.6  0.5  0:18.21 /usr/lib/x86_64-li
  1266 sir        20   0  449M 42124 31780 S   0.6  0.7  0:00.64 /usr/lib/x86_64-li
 33494 sir        20   0  461M 99888 84676 S   0.6  1.6  0:00.37 /usr/bin/qterminal
     1 root       20   0 22600 13132  9804 S   0.0  0.2  0:01.34 /sbin/init splash
   360 root       20   0 51416 16624 15360 S   0.0  0.3  0:00.29 /usr/lib/systemd/s
   402 root       20   0 29336  7768  4952 S   0.0  0.1  0:00.17 /usr/lib/systemd/s
   458 root       20   0  8276  7456  1664 S   0.0  0.1  0:00.30 /usr/sbin/haveged
   579 root       20   0  304M  9272  6600 S   0.0  0.2  0:00.06 /usr/libexec/accou
   580 root       20   0  7048  2560  2304 S   0.0  0.0  0:00.01 /usr/sbin/cron -f
   581 messagebus 20   0 10740  5888  4224 S   0.0  0.1  0:02.15 /usr/bin/dbus-daem
   583 polkitd    20   0  375M  9992  7476 S   0.0  0.2  0:00.20 /usr/lib/polkit-1/
   584 root       20   0 19052  8704  7680 S   0.0  0.1  0:00.11 /usr/lib/systemd/s
   605 root       20   0  304M  9272  6600 S   0.0  0.2  0:00.00 /usr/libexec/accou
   606 root       20   0  304M  9272  6600 S   0.0  0.2  0:00.00 /usr/libexec/accou
   620 root       20   0  304M  9272  6600 S   0.0  0.2  0:00.01 /usr/libexec/accou
   628 root       20   0  328M 23144 18276 S   0.0  0.4  0:00.13 /usr/sbin/NetworkM
   636 polkitd    20   0  375M  9992  7476 S   0.0  0.2  0:00.00 /usr/lib/polkit-1/
   637 polkitd    20   0  375M  9992  7476 S   0.0  0.2  0:00.00 /usr/lib/polkit-1/
F1Help  F2Setup F3SearchF4FilterF5Tree  F6SortByF7Nice -F8Nice +F9Kill  F10Quit
```

35. **Display a tree of all running processes.**

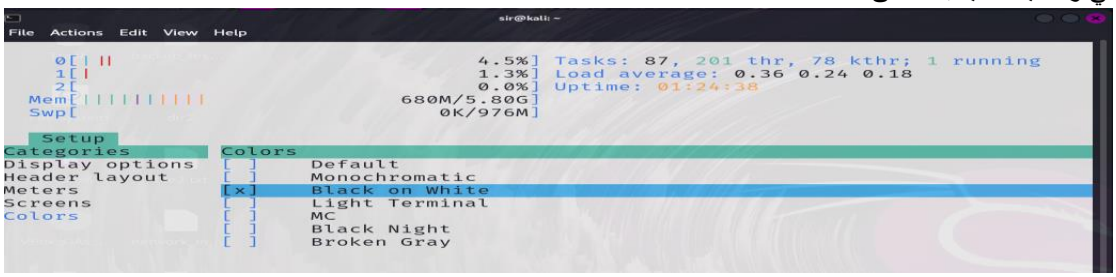
عرض شجرة العمليات الجارية:

```
sir@kali: ~
File  Actions  Edit  View  Help

┌──(sir㉿kali)-[~]
└─$ pstree
systemd─┬─ModemManager───3*[{ModemManager}]
        ├─NetworkManager───3*[{NetworkManager}]
        ├─3*[VBoxClient───VBoxClient───3*[{VBoxClient}]]
        ├─VBoxClient───VBoxClient───4*[{VBoxClient}]
        ├─VBoxDRMClient───4*[{VBoxDRMClient}]
        ├─VBoxService───8*[{VBoxService}]
        ├─accounts-daemon───3*[{accounts-daemon}]
        ├─agetty
        ├─colord───3*[{colord}]
```

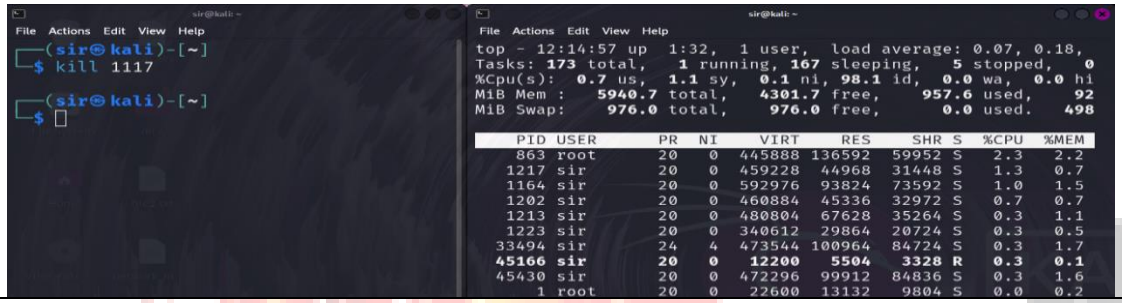
36. **Open the interactive process viewer and identify a process by its PID.**

فتح عارض العمليات التفاعلي وتحديد عملية بناءً على PID:



37. **Kill a process with a specific PID.**

قتل عملية معينة باستخدام PID:

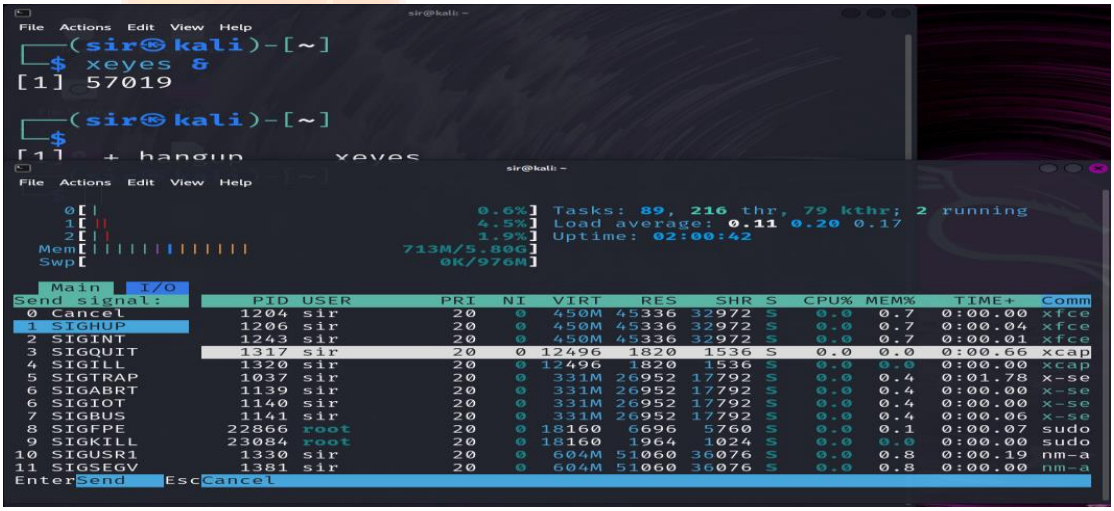


38. **Start an application and stop it using a command that kills processes by name(exeyes).**

بدء تطبيق وإيقافه باستخدام أمر يقتل العمليات بالاسم (exeyes):

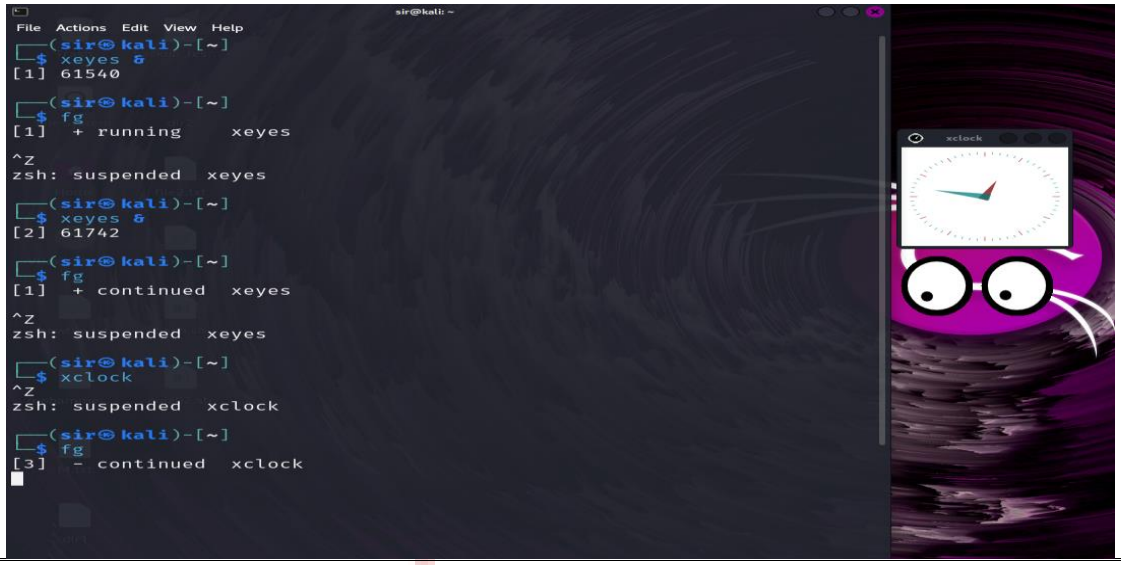
39. **Restart the application, then stop it using the interactive process viewer.**

إعادة تشغيل التطبيق، ثم إيقافه باستخدام عارض العمليات التفاعلي:



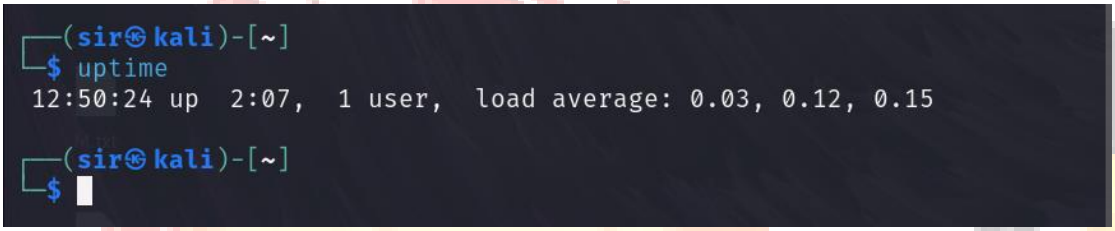
40. **Run a command in the background, then bring it to the foreground(exeyes).**

تشغيل أمر في الخلفية، ثم إحضاره إلى المقدمة (exeyes):



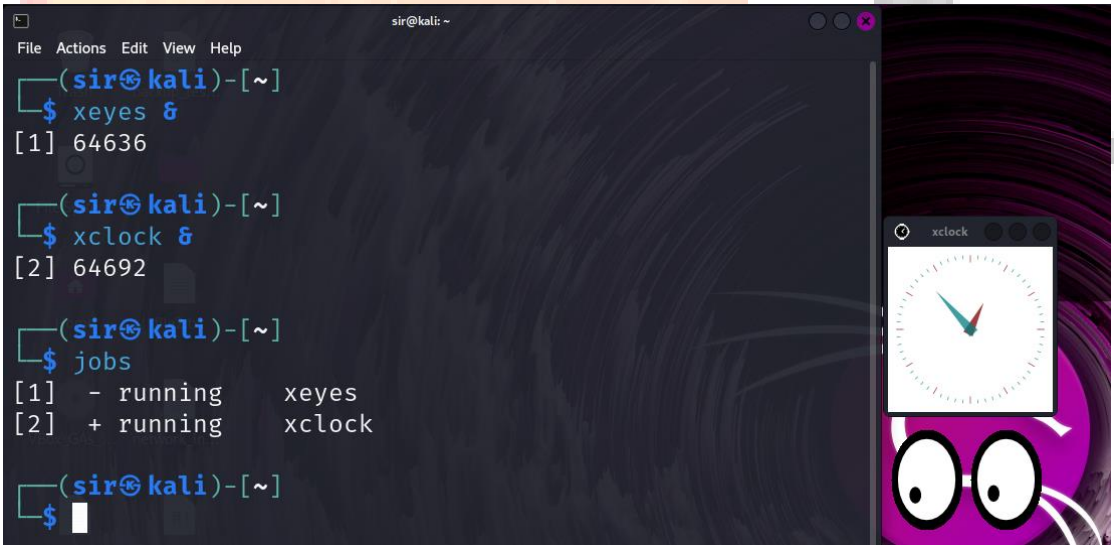
41. **Check how long the system has been running.**

التحقق من مدة تشغيل النظام:



42. **List all jobs running in the background.**

عرض جميع الوظائف الجارية في الخلفية:



SECTION 5: NETWORKING COMMANDS

43. **Display the network configuration.**

عرض إعدادات الشبكة:

- Ifconfig

```
sir@kali: ~
File  Actions  Edit  View  Help

┌──(sir㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe72:27cb  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:72:27:cb  txqueuelen 1000  (Ethernet)
        RX packets 9030  bytes 12446654 (11.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5988  bytes 398325 (388.9 KiB)
        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 9  bytes 578 (578.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 9  bytes 578 (578.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(sir㉿kali)-[~]
└─$
```

- Ip a

```
┌──(sir㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:72:27:cb brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 80397sec preferred_lft 80397sec
    inet6 fe80::a00:27ff:fe72:27cb/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

44. **Check the IP address of your machine.**

التحقق من عنوان IP للجهاز:

```
┌──(sir㉿kali)-[~]
└─$ hostname -I
10.0.2.15

┌──(sir㉿kali)-[~]
└─$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:72:27:cb brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 80235sec preferred_lft 80235sec
    inet6 fe80::a00:27ff:fe72:27cb/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(sir㉿kali)-[~]
```

45. **Test connectivity to an external server.**

اختبار الاتصال بسيرفر خارجي:

```
sir@kali: ~
File  Actions  Edit  View  Help

┌──(sir㉿kali)-[~]
└─$ ping example.com
PING example.com (93.184.215.14) 56(84) bytes of data.
64 bytes from 93.184.215.14: icmp_seq=1 ttl=53 time=808 ms
64 bytes from 93.184.215.14: icmp_seq=2 ttl=53 time=301 ms
64 bytes from 93.184.215.14: icmp_seq=3 ttl=53 time=210 ms
64 bytes from 93.184.215.14: icmp_seq=4 ttl=53 time=233 ms
64 bytes from 93.184.215.14: icmp_seq=5 ttl=53 time=253 ms
64 bytes from 93.184.215.14: icmp_seq=6 ttl=53 time=302 ms
64 bytes from 93.184.215.14: icmp_seq=7 ttl=53 time=277 ms
64 bytes from 93.184.215.14: icmp_seq=8 ttl=53 time=195 ms
64 bytes from 93.184.215.14: icmp_seq=9 ttl=53 time=233 ms
64 bytes from 93.184.215.14: icmp_seq=10 ttl=53 time=248 ms
64 bytes from 93.184.215.14: icmp_seq=11 ttl=53 time=284 ms
64 bytes from 93.184.215.14: icmp_seq=12 ttl=53 time=295 ms
```

46. **Display the routing table.**

عرض جدول التوجيه:

```
┌──(sir㉿kali)-[~]
└─$ ip route show
default via 10.0.2.2 dev eth0 proto dhcp src 10.0.2.15 metric 100
10.0.2.0/24 dev eth0 proto kernel scope link src 10.0.2.15 metric 100

┌──(sir㉿kali)-[~]
└─$
```

47. **Check the open ports and active connections.**

التحقق من المنافذ المفتوحة والاتصالات النشطة:

```
┌──(sir㉿kali)-[~]
└─$ netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State

┌──(sir㉿kali)-[~]
└─$ ss -tuln
Netid  State   Recv-Q   Send-Q     Local Address:Port     Peer Address:Port
```

48. **Show the IP address of the host machine and the VM, and verify if they are on the same network.**

عرض عنوان IP للجهاز والمضيف، والتحقق مما إذا كانا في نفس الشبكة:

```
┌──(sir㉿kali)-[~]
└─$ hostname -I
10.0.2.15

┌──(sir㉿kali)-[~]
└─$
```

```
C:\Program Files (x86)\VMware\VMware Workstation\bin>ping 10.0.2.15

Pinging 10.0.2.15 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.0.2.15:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

49. **Trace the route to an external server.**

تتبع المسار إلى سيرفر خارجي :

```
sir@kali: ~
File  Actions  Edit  View  Help

┌──(sir㉿kali)-[~]
└─$ traceroute 10.0.2.1
traceroute to 10.0.2.1 (10.0.2.1), 30 hops max, 60 byte packets
 1  10.0.2.15 (10.0.2.15)  3069.837 ms !H  3069.779 ms !H  3069.724 ms !H

┌──(sir㉿kali)-[~]
└─$ traceroute example.com
traceroute to example.com (93.184.215.14), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  0.988 ms  0.934 ms  0.887 ms
 2  10.0.2.2 (10.0.2.2)  17.897 ms  17.812 ms  17.888 ms
```

50. **Find out the default gateway.**

التحقق من بوابة العبور الافتراضية:

```
File  Actions  Edit  View  Help
┌──(sir㉿kali)-[~]
└─$ ip route | grep default
default via 10.0.2.2 dev eth0 proto dhcp src 10.0.2.15 metric 100

┌──(sir㉿kali)-[~]
└─$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.0.2.2        0.0.0.0         UG    100    0        0 eth0
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 eth0

┌──(sir㉿kali)-[~]
└─$
```

51. **Check the MAC address of your network interface.**

التحقق من عنوان MAC لواجهة الشبكة:

```
┌──(sir㉿kali)-[~]
└─$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
    link/ether 08:00:27:72:27:cb brd ff:ff:ff:ff:ff:ff
```

52. **Ensure that the VM can access external networks.**

التأكد من أن الجهاز الافتراضي يمكنه الوصول إلى الشبكات الخارجية:

```
File  Actions  Edit  View  Help
┌──(sir㉿kali)-[~]
└─$ 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=1 ttl=113 time=116 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=113 time=116 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=113 time=116 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=113 time=117 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=113 time=117 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=113 time=118 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=113 time=117 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=113 time=116 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=113 time=117 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=113 time=117 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=113 time=116 ms
64 bytes from 8.8.8.8: icmp_seq=12 ttl=113 time=117 ms
```

SECTION 6: UFW FIREWALL

53. **Enable the firewall.**

تمكين الجدار الناري:

```
┌──(sir㉿kali)-[~]
└─$ ufw --version
ufw 0.36.2
Copyright 2008-2023 Canonical Ltd.

┌──(sir㉿kali)-[~]
└─$ sudo ufw enable
Firewall is active and enabled on system startup

┌──(sir㉿kali)-[~]
└─$
```

54. **Allow SSH connections through the firewall.**

السماح باتصالات SSH من خلال الجدار الناري:

```
┌──(sir㉿kali)-[~]
└─$ sudo ufw allow ssh
Rule added
Rule added (v6)
```

55. **Deny all incoming traffic by default.**

حظر جميع الحركات الواردة بشكل افتراضي:

```
sir@kali: ~
File  Actions  Edit  View  Help

┌──(sir㉿kali)-[~]
└─$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)

┌──(sir㉿kali)-[~]
└─$
```

56. **Allow HTTP and HTTPS traffic.**

السماح بحركة HTTP وHTTPS:

```
┌──(sir㉿kali)-[~]
└─$ sudo ufw allow http
Rule added
Rule added (v6)

┌──(sir㉿kali)-[~]
└─$ sudo ufw allow https
Rule added
Rule added (v6)

┌──(sir㉿kali)-[~]
└─$
```

57. **Allow port 20.**

السماح بالاتصالات عبر المنفذ 20:

```
┌──(sir㉿kali)-[~]
└─$ sudo ufw allow 20
Rule added
Rule added (v6)
```

58. **Reset the firewall settings.**

إعادة تعيين إعدادات الجدار الناري:

```
┌──(sir㉿kali)-[~]
└─$ sudo ufw reset
Resetting all rules to installed defaults. Proceed with
operation (y|n)?
```

59. **Delete a rule from the firewall.**

حذف قاعدة من قواعد الجدار الناري:

```
┌──(sir㉿kali)-[~]
└─$ sudo ufw delete 1
```

60. **Disable the firewall.**

تعطيل الجدار الناري:

```
┌──(sir㉿kali)-[~]
└─$ sudo ufw disable
```

61. **View the status of the firewall.**

عرض حالة الجدار الناري:

```
┌──(sir㉿kali)-[~]
└─$ sudo ufw status
```

62. **Log firewall activity and view it.**

تسجيل نشاطات الجدار الناري وعرضها:

```
┌──(sir㉿kali)-[~]
└─$ sudo ufw logging on
```

SECTION 7: SEARCHING AND SYSTEM INFORMATION

63. **Delete the command history.**

حذف تاريخ الأوامر:

```
┌──(sir㉿kali)-[~/Desktop]
└─$ history -c
fc: event not found: -c
```

64. **Search for a kali in the `/etc/passwd` file.**

البحث عن كلمة "kali" في ملف `etc/passwd/`:

```
┌──(sir㉿kali)-[~/Desktop]
└─$ grep kali /etc/passwd

┌──(sir㉿kali)-[~/Desktop]
└─$ grep kali /etc/passwd
```

65. **Search for a kali in the `/etc/group` file.**

البحث عن كلمة "kali" في ملف `etc/group/`:

```
┌──(sir㉿kali)-[~/Desktop]
└─$ grep kali /etc/group
kali-trusted:x:135:
```

66. **Locate the `passwd` file.**

تحديد موقع ملف `passwd`:

```
┌──(sir㉿kali)-[~/Desktop]
└─$ which passwd
/usr/bin/passwd
```

67. **Locate the shadow file and open it.**

تحديد موقع ملف `shadow` وفتحه:

```
┌──(sir㉿kali)-[~/Desktop]
└─$ sudo cat /etc/shadow
root:!:19882:0:99999:7:::
daemon:*:19882:0:99999:7:::
bin:*:19882:0:99999:7:::
sys:*:19882:0:99999:7:::
sync:*:19882:0:99999:7:::
```

68. **Search for all configuration files in the `/etc` directory.**

البحث عن جميع ملفات التكوين في مجلد `/etc`:

```
┌──(sir㉿kali)-[~/Desktop]
└─$ find /etc -type f -name "*.conf"
/etc/mke2fs.conf
/etc/smartd.conf
/etc/miredo.conf
/etc/UPower/UPower.conf
```

69. **Search recursively for a specific word in the `/var/log` directory.**

البحث بشكل تكراري عن كلمة معينة في مجلد `var/log/`:

```
┌──(sir㉿kali)-[~/Desktop]
└─$ grep -r "var" /var/log
/var/log/Xorg.0.log.old:[     7.181] (==) Log file: "/var/log/Xorg.0.log", Time: Sat Aug 31 23:42:38 2024
grep: /var/log/boot.log.4: Permission denied
grep: /var/log/lightdm: Permission denied
grep: /var/log/boot.log.1: Permission denied
grep: /var/log/boot.log.2: Permission denied
grep: /var/log/speech-dispatcher: Permission denied
grep: /var/log/boot.log: Permission denied
grep: /var/log/inetsim: Permission denied
grep: /var/log/vboxadd-install.log: Permission denied
/var/log/Xorg.1.log.old:[  2383.961] (==) Log file: "/var/log/Xorg.1.log", Time: Wed Aug  7 18:28:01 2024
```

70. **View the system's kernel version.**

عرض إصدار نواة النظام:

```
┌──(sir㉿kali)-[~/Desktop]
└─$ uname -r
6.6.15-amd64
```

71. **Display the system's memory usage.**

عرض استخدام الذاكرة في النظام:

```
┌──(sir㉿kali)-[~/Desktop]
└─$ free -h
              total        used        free      shared  buff/cache   available
Mem:          5.8Gi       1.0Gi       3.9Gi       9.4Mi       1.2Gi       4.8Gi
Swap:         975Mi          0B       975Mi
```

72. **Show the system's disk usage.**

عرض استخدام القرص في النظام:

```
┌──(sir㉿kali)-[~/Desktop]
└─$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            2.9G     0  2.9G   0% /dev
tmpfs           595M  1.1M  594M   1% /run
/dev/sda1        49G   15G   32G  32% /
tmpfs           3.0G     0  3.0G   0% /dev/shm
```

73. **Check the system's uptime and load average.**

لتحقق من وقت تشغيل النظام ومتوسط الحمل:

```
┌──(sir㉿kali)-[~/Desktop]
└─$ uptime
 14:54:32 up  4:11,  1 user,  load average: 0.00, 0.03, 0.01
```

74. **Display the current logged-in users.**

عرض المستخدمين الحاليين المسجلين في النظام:

```
┌──(sir㉿kali)-[~/Desktop]
└─$ who
sir      tty7         2024-09-01 10:43 (:0)
sir      pts/1        2024-09-01 11:28
sir      pts/3        2024-09-01 14:18
sir      pts/4        2024-09-01 14:20
sir      pts/5        2024-09-01 14:22
sir      pts/6        2024-09-01 14:29
sir      pts/7        2024-09-01 14:30
sir      pts/8        2024-09-01 14:31
sir      pts/9        2024-09-01 14:33
sir      pts/10       2024-09-01 14:34
```

75. **Check the identity of the current user.**

التحقق من هوية المستخدم الحالي:

```
┌──(sir㉿kali)-[~/Desktop]
└─$ whoami
sir
```

76. **View the `/var/log/auth.log` file.**

عرض ملف `var/log/auth.log/`:

```
┌──(sir㉿kali)-[~/Desktop]
└─$ sudo less /var/log/auth.log
/var/log/auth.log: No such file or directory
```

77. **Shred the `auth.log` file securely.**

تقطيع ملف `auth.log` بشكل آمن:

```
┌──(sir㉿kali)-[~/Desktop]
└─$ sudo shred -u /var/log/auth.log
shred: /var/log/auth.log: failed to open for writing: No such file or directory
```

78. **How do you lock a user account to prevent them from logging in.**

كيفية قفل حساب مستخدم لمنعه من تسجيل الدخول:

```
┌──(sir㉿kali)-[~/Desktop]
└─$ sudo usermod -L sir
```

79. **What command would you use to change a user's default shell.**

تغيير الصدفة الافتراضية لمستخدم:

```
┌──(sir㉿kali)-[~/Desktop]
└─$ sudo chsh -s /bin/bash sir
```

80. **Display the system's boot messages.**

عرض رسائل الإقلاع للنظام:

```
sir@kali: ~/Desktop
File  Actions  Edit  View  Help
[    0.000000] Linux version 6.6.15-amd64 (devel@kali.org) (gcc-13 (Debian 13.2.0
-24) 13.2.0, GNU ld (GNU Binutils for Debian) 2.42) #1 SMP PREEMPT_DYNAMIC Kali 6
.6.15-2kali1 (2024-05-17)
[    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-6.6.15-amd64 root=UUID=87d2
f760-2ba2-47f1-965c-12ab19f8ce3c ro quiet splash
[    0.000000] [Firmware Bug]: TSC doesn't count with P0 frequency!
[    0.000000] BIOS-provided physical RAM map:
[    0.000000] BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
[    0.000000] BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000000100000-0x00000000dffeffff] usable
[    0.000000] BIOS-e820: [mem 0x00000000dfff0000-0x00000000dfffffff] ACPI data
[    0.000000] BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000100000000-0x00000001a07fffff] usable
[    0.000000] NX (Execute Disable) protection: active
[    0.000000] APIC: Static calls initialized
[    0.000000] SMBIOS 2.5 present.
[    0.000000] DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/200
6
[    0.000000] Hypervisor detected: KVM
[    0.000000] kvm-clock: Using msrs 4b564d01 and 4b564d00
[    0.000002] kvm-clock: using sched offset of 9922726103 cycles
[    0.000005] clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd
42e4dffb, max_idle_ns: 881590591483 ns
[    0.000007] tsc: Detected 2295.686 MHz processor
[    0.001263] e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
[    0.001266] e820: remove [mem 0x000a0000-0x000fffff] usable
[    0.001271] last_pfn = 0x1a0800 max_arch_pfn = 0x400000000
[    0.001281] MTRRs disabled by BIOS
[    0.001283] x86/PAT: Configuration [0-7]: WB  WC  UC- UC  WB  WP  UC- WT
[    0.001304] last_pfn = 0xdfff0 max_arch_pfn = 0x400000000
[    0.001327] found SMP MP-table at [mem 0x0009fff0-0x0009ffff]
[    0.001620] RAMDISK: [mem 0x2e8a3000-0x33448fff]
log file: S
```

تم بحمد الله

Prepared By Eng.	**Alshebli Fisal Ahmeb Al-Shebli**
Subject	**Cyber Security**
Subject teacher	**Eng. Abdulrazzaq Al-Samawi**