التكليف الثاني الكالي لينكس

1. Display the current working directory.

###1.عرض الدليل الحالي.

```
┌──(kali㉿kali)-[~]
└─$ pwd
/home/kali
```

****
****

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

###2. إدراج جميع محتويات الدليل الحالي، بما في ذلك الملفات المخفية.

```
┌──(kali㉿kali)-[~]
└─$ ls -la
total 124
drwxr-xr-x 15 kali kali  4096 Sep 24 13:03 .
drwxr-xr-x  3 root root  4096 Sep 23 17:26 ..
-rw-r--r--  1 kali kali   220 Sep 23 17:26 .bash_logout
-rw-r--r--  1 kali kali  5551 Sep 23 17:26 .bashrc
-rw-r--r--  1 kali kali  3526 Sep 23 17:26 .bashrc.original
drwx------  9 kali kali  4096 Sep 24 13:03 .cache
drwxr-xr-x 14 kali kali  4096 Sep 24 13:03 .config
drwxr-xr-x  3 kali kali  4096 Sep 24 13:00 Desktop
-rw-r--r--  1 kali kali    35 Sep 23 17:29 .dmrc
drwxr-xr-x  2 kali kali  4096 Sep 23 17:29 Documents
drwxr-xr-x  2 kali kali  4096 Sep 23 17:29 Downloads
-rw-r--r--  1 kali kali 11759 Sep 23 17:26 .face
lrwxrwxrwx  1 kali kali     5 Sep 23 17:26 .face.icon -> .face
drwx------  3 kali kali  4096 Sep 23 17:29 .gnupg
-rw-------  1 kali kali     0 Sep 23 17:29 .ICEauthority
drwxr-xr-x  3 kali kali  4096 Sep 23 17:26 .java
drwxr-xr-x  3 kali kali  4096 Sep 23 17:29 .local
drwxr-xr-x  2 kali kali  4096 Sep 23 17:29 Music
drwxr-xr-x  2 kali kali  4096 Sep 24 13:04 Pictures
```

****
****

3. Change your directory to the `Desktop`.

###3. تغيير الدليل إلى `Desktop`.

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

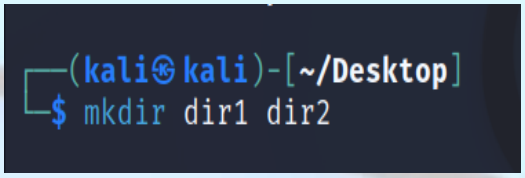
Or:

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

****
****

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

###4.على سطح المكتب `dir2` و `dir1` إنشاء دليلين باسم.



****
****

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

###5. `file1.txt` ، إنشاء ملف باسم`dir1` داخل.

****
****

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

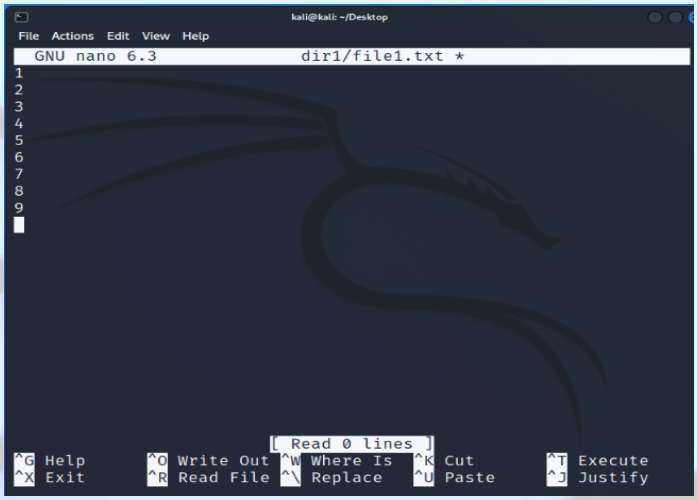
###6. `file2.txt` ، إنشاء ملف باسم`dir2` داخل.

****
****

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

###7. `file1.txt` ، اكتب الأرقام من ١ إلى ٩ في **vim** أو **nano** باستخدام.

الادخال:



احفظ واخرج باستخدام `CTRL + X` ، ثم `Y` و`Enter`.

****

****

8. From the home directory, copy the contents of `file1.txt` into `file2.txt`.

###8. من الدليل الرئيسي، انسخ محتويات `file1.txt` إلى `file2.txt`.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ cp dir1/file1.txt dir2/file2.txt
```

****
****

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

###9. من الدليل الرئيسي، احذف `file1.txt` داخل `dir1`.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ rm dir1/file1.txt
```

****
****

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

###10. إزالة الدليل `dir1` من سطح المكتب.

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

****
****

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

###11.على سطح المكتب `network_info.txt` قم بإعادة توجيه ناتج أمر تكوين الشبكة إلى ملف باسم.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ifconfig > ~/Desktop/network_info.txt
```

****
****

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

###12.افتح مجلد سطح المكتب وأظهر جميع الملفات بمعلومات مفصلة.

```
┌──(kali㉿kali)-[~]
└─$ ls -la ~/Desktop
total 28
drwxr-xr-x  4 kali kali 4096 Sep 24 18:34 .
drwxr-xr-x 16 kali kali 4096 Sep 24 15:25 ..
drwxr-xr-x  2 kali kali 4096 Sep 24 15:07 dir2
-rw-r--r--  1 kali kali   18 Sep 24 15:28 file1.txt
-rw-r--r--  1 kali kali    9 Sep 24 15:25 file2.txt
-rw-r--r--  1 kali kali  871 Sep 24 18:34 network_info.txt
drwxrwxrwx  2 kali kali 4096 Sep 24 12:55 الكالي
```

****
****

13. Create a new user with your name.

###13.إنشاء مستخدم جديد باسمك.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo adduser kawther
[sudo] password for kali:
Sorry, try again.
```

****
****

14. Set a password for your user.

###14.تعيين كلمة مرور لمستخدمك.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo passwd kawther
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.

###15.افتح الملف الذي يحتوي على معلومات المستخدم وتحقق من إضافة مستخدمك.

```
┌──(kali㉿kali)-[~]
└─$ cat /etc/passwd | grep kawther
kawther:x:1001:1001:,,,:/home/kawther:/bin/bash
```

****
****

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

###16.أضف مستخدمك إلى الملف الذي يمنح صلاحيات إدارية.

```
┌──(kali㉿kali)-[~]
└─$ sudo usermod -aG sudo kawther
[sudo] password for kali:
```

****
****

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

_To switch to the user use:

```
┌──(kali㉿kali)-[~]
└─$ su - kawther
Password:
┌──(kawther㉿kali)-[~]
└─$
```

_To confirm the user identity, use:

```
┌──(kawther㉿kali)-[~]
└─$ whoami
kawther
```

###17.انتقل إلى مستخدمك وتحقق من هوية المستخدم.

_للانتقال إلى المستخدم نستخدم:

```
┌──(kali㉿kali)-[~]
└─$ su - kawther
Password:
┌──(kawther㉿kali)-[~]
└─$
```

_للتأكد من هوية المستخدم، نستخدم:

```
┌──(kawther㉿kali)-[~]
└─$ whoami
kawther
```

****
****

18. Create a new group named `testgroup`.

###18.إنشاء مجموعة جديدة باسم `testgroup` .

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

****
****

19. Add your user to `testgroup`.

###19.أضف مستخدمك إلى `testgroup`.

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

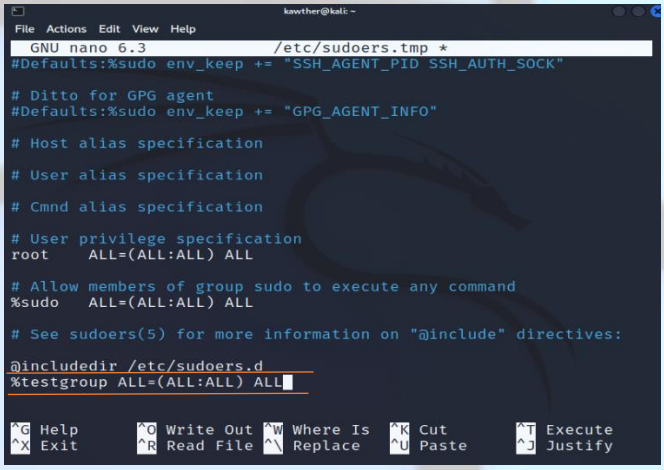
****
****

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

_To give administrative privileges to the group **"testgroup"**, you can edit the **sudoers** file using:

```
┌──(kawther㉿kali)-[~]
└─$ sudo visudo
```

_Then add the following line:

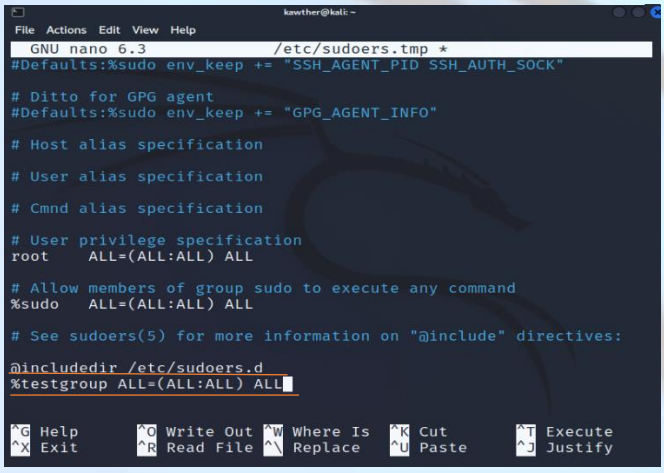


20. إلى الملف الذي يمنح صلاحيات إدارية `testgroup` أضف المجموعة .

_باستخدام **sudoers** ، يمكنك تعديل ملف **"testgroup"** لإعطاء صلاحيات إدارية للمجموعة.

```
┌──(kawther㉿kali)-[~]
└─$ sudo visudo
```

ثم أضف السطر التالي:



****
****

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

###21. إزالة مستخدمك من الملف الذي يمنح صلاحيات إدارية.

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

****
****

22. Check if your user still has administrative privileges.

###22. تحقق مما إذا كان مستخدمك لا يزال لديه صلاحيات إدارية.

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

****
****

23. Check which groups your user belongs to.

###23. تحقق من المجموعات التي ينتمي إليها مستخدمك.

```
┌──(kawther㉿kali)-[~]
└─$ groups
kawther sudo
```

****
****

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.

###٢٤. على سطح المكتب للسماح للمالك بالقراءة والكتابة والتنفيذ؛ والمجموعة بالقراءة والتنفيذ؛ **`file2.txt`** تعيين الأذونات لـ والآخرين بالقراءة.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ chmod 751 ~/Desktop/file2.txt
```

****
****

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

###25. للتحقق من التغيير `file2.txt` تحقق من الأذونات لـ

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls -l ~/Desktop/file2.txt
-rwxr-x--x 1 kali kali 9 Sep 24 15:25 /home/kali/Desktop/file2.txt
```

****
****

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

###26. إلى مستخدمك `file2.txt` تغيير ملكية.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo chown kawther ~/Desktop/file2.txt
[sudo] password for kali:
```

****
****

27. Verify the ownership of `file2.txt`.

###27. `file2.txt` تحقق من ملكية.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls -l ~/Desktop/file2.txt
-rwxr-x--x 1 kawther kali 9 Sep 24 15:25 /home/kali/Desktop/file2.txt
```

****
****

28. Change back the ownership of `file2.txt`.

###28. إلى المستخدم الأصلي `file2.txt` إعادة تغيير ملكية.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo chown kali ~/Desktop/file2.txt
```

****
****

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

###29. منح إذن الكتابة للجميع لـ `file2.txt`

```
┌──(kali㉿kali)-[~/Desktop]
└─$ chmod a+w ~/Desktop/file2.txt
```

****
****

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

###30. إزالة إذن الكتابة للمجموعة والآخرين لـ `file2.txt`

```
┌──(kali㉿kali)-[~/Desktop]
└─$ chmod go+w ~/Desktop/file2.txt
```

****
****

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

###31. بعد إجراء التغييرات اللازمة على الملكية والأذونات حذف `file2.txt`.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ rm ~/Desktop/file2.txt
```

****
****

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

###32. إلى `٧٥٥` ؟`project` ما هو الأمر الذي ستستخدمه لتغيير الأذونات بشكل تكراري لجميع الملفات والدلائل داخل مجلد يسمى

```
┌──(kali㉿kali)-[~/Desktop]
└─$ chmod -R 755 ~/project
chmod: cannot access '/home/kali/project': No such file or directory
```

****
****

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

###33.(**htop**) تثبيت أداة مراقبة النظام التي توفر عارض عمليات تفاعلي.

```
┌──(kali㉿kali)-[~]
└─$ sudo apt update && sudo apt install htop
[sudo] password for kali:
Ign:1 http://http.kali.org/kali kali-rolling InRelease
Ign:1 http://http.kali.org/kali kali-rolling InRelease
Ign:1 http://http.kali.org/kali kali-rolling InRelease
Err:1 http://http.kali.org/kali kali-rolling InRelease
  Could not resolve 'http.kali.org'
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
```

_use the following command (for **Debian**-based systems like Ubuntu):

_(مثل أوبونتو **Debian** لأنظمة)، نستخدم الأمر:

****
****

34. Display all running processes.

###34.عرض جميع العمليات الجارية.

```
┌──(kali㉿kali)-[~]
└─$ ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.6 167976 12020 ?        Ss   16:28   0:03 /sbin/init splash
root           2  0.0  0.0      0     0 ?        S    16:28   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   16:28   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   16:28   0:00 [rcu_par_gp]
root           5  0.0  0.0      0     0 ?        I<   16:28   0:00 [netns]
root           7  0.0  0.0      0     0 ?        I<   16:28   0:00 [kworker/0:0H-events_highpri]
root           9  0.0  0.0      0     0 ?        I<   16:28   0:01 [kworker/0:1H-events_highpri]
root          10  0.0  0.0      0     0 ?        I<   16:28   0:00 [mm_percpu_wq]
root          11  0.0  0.0      0     0 ?        I    16:28   0:00 [rcu_tasks_kthread]
root          12  0.0  0.0      0     0 ?        I    16:28   0:00 [rcu_tasks_rude_kthread]
root          13  0.0  0.0      0     0 ?        I    16:28   0:00 [rcu_tasks_trace_kthread]
root          14  0.0  0.0      0     0 ?        S    16:28   0:00 [ksoftirqd/0]
root          15  0.0  0.0      0     0 ?        I    16:28   0:11 [rcu_preempt]
```

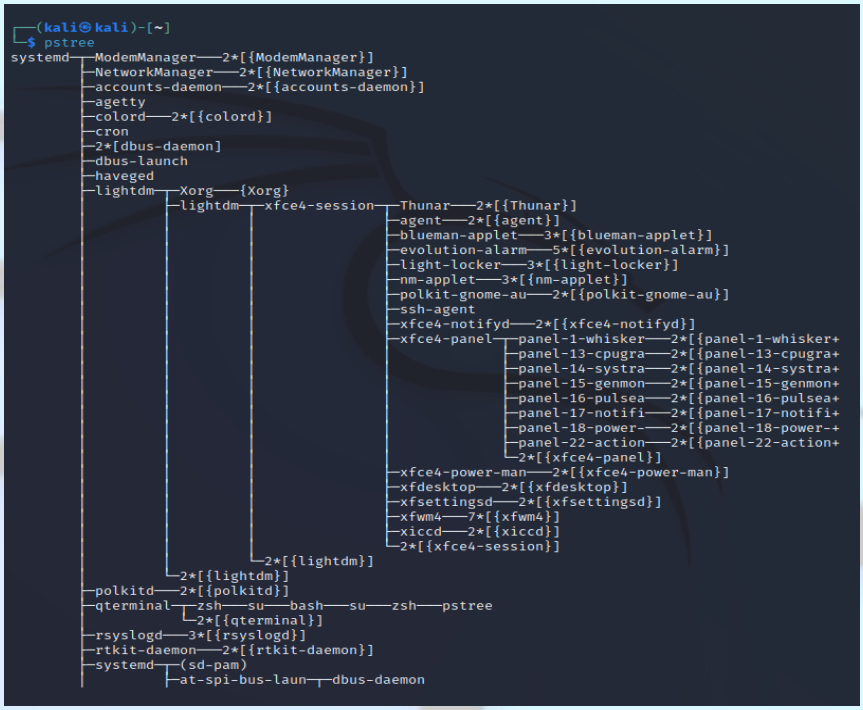
Or:

```
┌──(kali㉿kali)-[~]
└─$ ps aux --forest
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           2  0.0  0.0      0     0 ?        S    16:28   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   16:28   0:00  \_ [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   16:28   0:00  \_ [rcu_par
root           5  0.0  0.0      0     0 ?        I<   16:28   0:00  \_ [netns]
root           7  0.0  0.0      0     0 ?        I<   16:28   0:00  \_ [kworker
root           9  0.0  0.0      0     0 ?        I<   16:28   0:01  \_ [kworker
root          10  0.0  0.0      0     0 ?        I<   16:28   0:00  \_ [mm_perc
root          11  0.0  0.0      0     0 ?        I    16:28   0:00  \_ [rcu_tas
root          12  0.0  0.0      0     0 ?        I    16:28   0:00  \_ [rcu_tas
root          13  0.0  0.0      0     0 ?        I    16:28   0:00  \_ [rcu_tas
root          14  0.0  0.0      0     0 ?        S    16:28   0:00  \_ [ksoftir
```

****
****

35. Display a tree of all running processes.

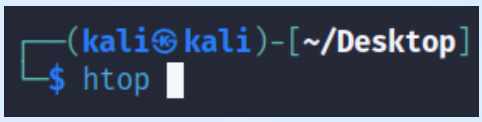
###35.عرض شجرة لجميع العمليات الجارية.

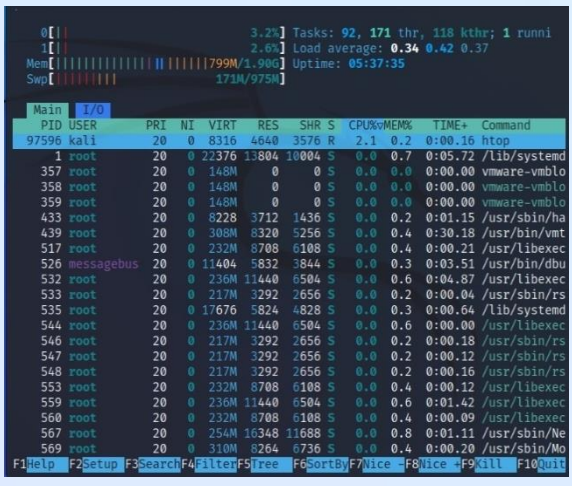


****
****

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

###36. افتح عارض العمليات التفاعلي وحدد عملية بواسطة الخاص بها **PID**.





****
****

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

###37. محدد **PID** إنهاء عملية بواسطة.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ kill 109314
```

****
****

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

_To start the `**xeyes**` application, use:

```
┌──(kali㉿kali)-[~]
└─$ xeyes &
[2] 207564
```

_To stop it, use:

```
┌──(kali㉿kali)-[~]
└─$ pkill xeyes
[2]   + terminated  xeyes

[1]   + terminated  xeyes
```

###38. (**xeyes**) ابدأ تطبيقًا وأوقفه باستخدام أمر يقتل العمليات حسب الاسم.

_استخدم`**xeyes**` للبدء في تطبيق:

```
┌──(kali㉿kali)-[~]
└─$ xeyes &
[2] 207564
```

_لإيقافه، استخدم:

```
┌──(kali㉿kali)-[~]
└─$ pkill xeyes
[2]   + terminated  xeyes

[1]   + terminated  xeyes
```

****
****

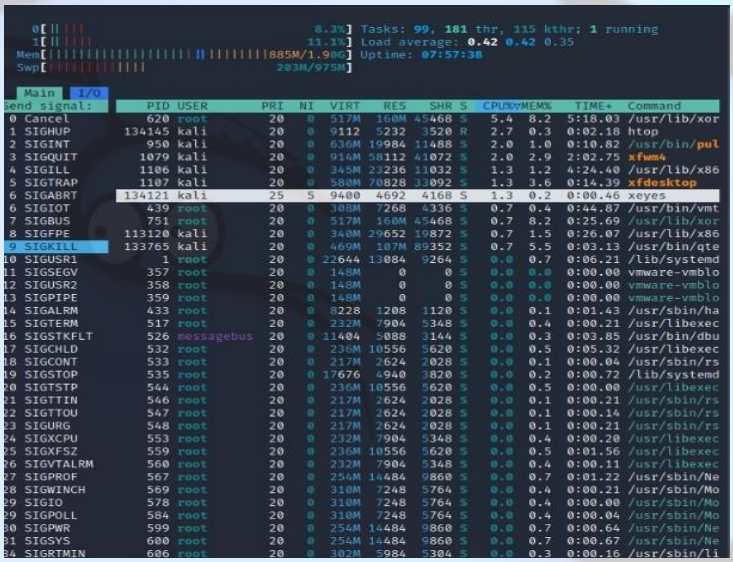
39. Restart the application, then stop it using the interactive process viewer.

_To restart `xeyes`, use:

```
┌──(kali㉿kali)-[~]
└─$ xeyes &
[1] 134121
```

_Then, open **`htop`**:

```
┌──(kali㉿kali)-[~]
└─$ htop
```



Find **`xeyes`** in the list, and use the F9 key to kill the process.

###39.أعد تشغيل التطبيق، ثم أوقفه باستخدام عارض العمليات التفاعلي.

_نستخدم**`xeyes`** لإعادة تشغيل:

```
┌──(kali㉿kali)-[~]
└─$ xeyes &
[1] 134121
```

_**`htop`** ثم، افتح:

```
┌──(kali㉿kali)-[~]
└─$ htop
```

وثم ١٥ او ٩, لقتل العملية **F9** في القائمة، واستخدم مفتاح **`xeyes`** ابحث عن.

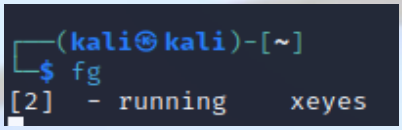
****
****

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

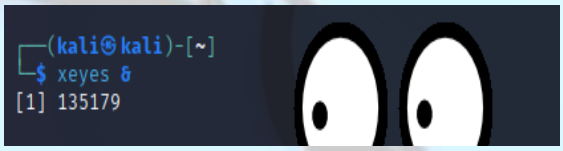
###40. (**xeyes**) قم بتشغيل أمر في الخلفية، ثم أحضره إلى المقدمة.

_To run `**xeyes**` in the background, use:

_To bring it to the foreground, use:



_في الخلفية، استخدم `**xeyes**` لتشغيل:

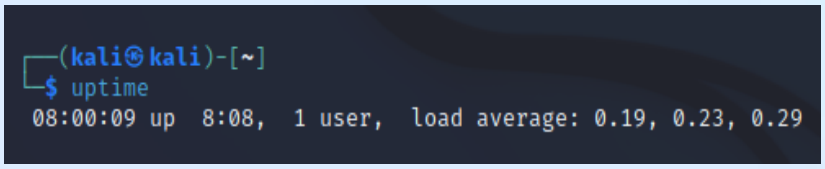


_لإحضاره إلى المقدمة، استخدم:

****
****

41. Check how long the system has been running.

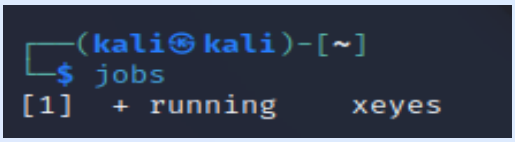
###41. تحقق من مدة تشغيل النظام.



****
****

42. List all jobs running in the background.

###42. إدراج جميع المهام الجارية في الخلفية.



****
****

43. Display the network configuration.

###43. عرض تكوين الشبكة.

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.88.130  netmask 255.255.255.0  broadcast 192.168.88.255
        inet6 fe80::20c:29ff:fe79:69c6  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:79:69:c6  txqueuelen 1000  (Ethernet)
        RX packets 138226  bytes 199168360 (189.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 52727  bytes 3455575 (3.2 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 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Or:

```
┌──(kali㉿kali)-[~]
└─$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default 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
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen
 1000
    link/ether 00:0c:29:79:69:c6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.88.130/24 brd 192.168.88.255 scope global dynamic noprefixroute eth0
       valid_lft 1221sec preferred_lft 1221sec
    inet6 fe80::20c:29ff:fe79:69c6/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

****
****

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

###44. لجهازك **IP** تحقق من عنوان.

```
┌──(kali㉿kali)-[~]
└─$ hostname -I
192.168.88.130
```

****
****

45. Test connectivity to an external server.

###45. اختبار الاتصال بخادم خارجي .

```
┌──(kali㉿kali)-[~]
└─$ ping google.com
PING google.com (142.251.143.206) 56(84) bytes of data.
64 bytes from trn06s04-in-f14.1e100.net (142.251.143.206): icmp_seq=1 ttl=128 time=197 ms
64 bytes from trn06s04-in-f14.1e100.net (142.251.143.206): icmp_seq=2 ttl=128 time=219 ms
64 bytes from trn06s04-in-f14.1e100.net (142.251.143.206): icmp_seq=3 ttl=128 time=240 ms
64 bytes from trn06s04-in-f14.1e100.net (142.251.143.206): icmp_seq=4 ttl=128 time=155 ms
64 bytes from trn06s04-in-f14.1e100.net (142.251.143.206): icmp_seq=5 ttl=128 time=111 ms
64 bytes from trn06s04-in-f14.1e100.net (142.251.143.206): icmp_seq=7 ttl=128 time=214 ms
64 bytes from trn06s04-in-f14.1e100.net (142.251.143.206): icmp_seq=8 ttl=128 time=129 ms
64 bytes from trn06s04-in-f14.1e100.net (142.251.143.206): icmp_seq=9 ttl=128 time=392 ms
64 bytes from trn06s04-in-f14.1e100.net (142.251.143.206): icmp_seq=10 ttl=128 time=181 ms
64 bytes from trn06s04-in-f14.1e100.net (142.251.143.206): icmp_seq=12 ttl=128 time=1232 ms
64 bytes from trn06s04-in-f14.1e100.net (142.251.143.206): icmp_seq=13 ttl=128 time=208 ms
64 bytes from trn06s04-in-f14.1e100.net (142.251.143.206): icmp_seq=14 ttl=128 time=230 ms
64 bytes from trn06s04-in-f14.1e100.net (142.251.143.206): icmp_seq=15 ttl=128 time=150 ms
64 bytes from trn06s04-in-f14.1e100.net (142.251.143.206): icmp_seq=16 ttl=128 time=173 ms
64 bytes from trn06s04-in-f14.1e100.net (142.251.143.206): icmp_seq=17 ttl=128 time=195 ms
64 bytes from trn06s04-in-f14.1e100.net (142.251.143.206): icmp_seq=18 ttl=128 time=423 ms
64 bytes from trn06s04-in-f14.1e100.net (142.251.143.206): icmp_seq=19 ttl=128 time=242 ms
64 bytes from trn06s04-in-f14.1e100.net (142.251.143.206): icmp_seq=20 ttl=128 time=162 ms
^C
── google.com ping statistics ──
20 packets transmitted, 18 received, 10% packet loss, time 19081ms
rtt min/avg/max/mdev = 110.908/269.614/1232.300/246.042 ms, pipe 2
```

This will send **ICMP** echo requests to check connectivity.

للتحقق من الاتصال **ICMP** سيقوم هذا بإرسال طلبات.

****
****

46. Display the routing table.

عرض جدول التوجيه.

```
┌──(kali㉿kali)-[~]
└─$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.88.2    0.0.0.0         UG    100    0        0 eth0
192.168.88.0    0.0.0.0         255.255.255.0   U     100    0        0 eth0
```

Or:

```
┌──(kali㉿kali)-[~]
└─$ ip route show
default via 192.168.88.2 dev eth0 proto dhcp src 192.168.88.130 metric 100
192.168.88.0/24 dev eth0 proto kernel scope link src 192.168.88.130 metric 100
```

****
****

47. Check the open ports and active connections.

###47. تحقق من المنافذ المفتوحة والاتصالات النشطة.

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

_For a more modern approach:

_لنهج أكثر حداثة:

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

****

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

###48. لجهاز المضيف والآلة الافتراضية، والتحقق مما إذا كانا على نفس الشبكة **IP** عرض عنوان.

1)**لجهاز المضيف الى هو جهازي. **IP** عرض عنوان:
_لجهاز المضيف **IP** كتابة الأمر للحصول على:

```
C:\Users\PC>ipconfig

Connection-specific DNS Suffix  . :
Link-local IPv6 Address . . . . . : fe80::617a:586b:b0aa:36ea%19
IPv4 Address. . . . . . . . . . . : 192.168.88.1
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . :
```

2)**لجهاز الآلة الافتراضية الي هي اللينكس. **IP** عرض عنوان:
_ لجهاز الآلة الافتراضية **IP** كتابة الامر للحصول على:

```
┌──(kali㉿kali)-[~]
└─$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNK
NOWN group default 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
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_co
del state UP group default qlen 1000
    link/ether 00:0c:29:79:69:c6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.88.130/24 brd 192.168.88.255 scope global dyna
mic noprefixroute eth0
       valid_lft 1797sec preferred_lft 1797sec
    inet6 fe80::20c:29ff:fe79:69c6/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

3)**التحقق مما إذا كانا على نفس الشبكة .

1. **IP** نقارن عناوين:

_ لجهاز المضيف و للآلة الافتراضية متشابهان في الجزء الأول **IP** نتأكد من أن عنوان.
_جهاز المضيف: **"192.168.88.1"**
_الآلة الافتراضية: **"192.168.88.130"**
_ اذا متشابهان في الجزاء الأول الي هو **"192.168.88"**
_لكلا الجهازين متطابقًا فإنهما على نفس الشبكة IP إذا كان الجزء الأول من عنوان.

2. نقارن قناع الشبكة:

_نتحقق من أن قناع الشبكة لكلا الجهازين هو نفسه:
"255.255.255.0"

****
****

49. Trace the route to an external server.

###49. تتبع المسار إلى خادم خارجي.

```
┌──(kali㉿kali)-[~]
└─$ traceroute google.com
traceroute to google.com (142.251.143.206), 30 hops max, 60 byte packets
 1  _gateway (192.168.88.2)  0.395 ms  0.292 ms  0.330 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
```

****
****

50. Find out the default gateway.

###50. اكتشاف البوابة الافتراضية.

```
┌──(kali㉿kali)-[~]
└─$ ip route | grep default
default via 192.168.88.2 dev eth0 proto dhcp src 192.168.88.130 metric 100
```

****
****

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

###51. لواجهة الشبكة الخاصة بك **MAC** تحقق من عنوان.

```
┌──(kali㉿kali)-[~]
└─$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEF
AULT 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 00:0c:29:79:69:c6 brd ff:ff:ff:ff:ff:ff
```

_This will display all network interfaces along with their **MAC** addresses.

_الخاصة بها **MAC** سيعرض هذا جميع واجهات الشبكة مع عناوين.

****
****

52. Ensure that the VM can access external networks.

###52. تأكد من أن الآلة الافتراضية يمكنها الوصول إلى الشبكات الخارجية.

```
┌──(kali㉿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=128 time=328 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=247 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=270 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=192 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=128 time=215 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=128 time=239 ms
^C
── 8.8.8.8 ping statistics ──
7 packets transmitted, 6 received, 14.2857% packet loss, time 6004ms
rtt min/avg/max/mdev = 191.820/248.508/327.560/43.107 ms
```

****
****

53. Enable the firewall.

###53. تفعيل جدار الحماية.

```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT
[sudo] password for kali:
```

****
****

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

###54.عبر جدار الحماية **SSH** السماح باتصالات.

```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

****
****

55. Deny all incoming traffic by default.

###55. رفض جميع حركة المرور الواردة بشكل افتراضي.

```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -p INPUT DROP
iptables v1.8.8 (nf_tables): unknown protocol "input" specified
Try `iptables -h' or 'iptables --help' for more information.
```

****
****

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

_Allow **HTTP** traffic:

```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

_Allow **HTTPS** traffic:

```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```

###56. **HTTPS** و **HTTP** السماح بحركة مرور.

_**HTTP** السماح بحركة مرور:

```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

_**HTTPS** السماح بحركة مرور:

```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```

****
****

57. Allow port 20.

###57. السماح بالمنفذ ٢٠

_Allow **TCP** traffic:

_**TCP**السماح بحركة:

```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -A INPUT -p tcp --dport 20 -j ACCEPT
```

****
****

58. Reset the firewall settings.

###58. إعادة تعيين إعدادات جدار الحماية إلى الإعدادات الافتراضية.

```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -F && sudo iptables -X && sudo iptables -P INPUT ACCEPT && sudo iptables -P FORWARD ACCEPT && sudo iptables -P OUTPUT ACCEPT
```

****
****

59. Delete a rule from the firewall.

###59. حذف قاعدة من جدار الحماية.

```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -D INPUT 3
iptables: Index of deletion too big.
```

****
****

60. Disable the firewall.

###60. تعطيل جدار الحماية.

```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -F && sudo iptables -P INPUT ACCEPT && sudo iptables -P FORWARD ACCEPT && sudo iptables -P OUTPUT ACCEPT
```

****
****

61. View the status of the firewall.

###61.عرض حالة جدار الحماية.

```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -L -v -n
Chain INPUT (policy ACCEPT 11 packets, 1259 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 1 packets, 310 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

****
****

62. Log firewall activity and view it.

_To enable logging for the firewall, use:

```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -A INPUT -j LOG --log-prefix "iptables-input: " --log-level 4
```

_To view the logs:

```
┌──(kali㉿kali)-[~]
└─$ sudo tail -f /var/log/syslog | grep "iptables-input"
[sudo] password for kali:
```

###62.تسجيل نشاط جدار الحماية وعرضه.

_لتمكين تسجيل لجدار الحماية:

```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -A INPUT -j LOG --log-prefix "iptables-input: " --log-level 4
```

_لعرض السجلات:

```
┌──(kali㉿kali)-[~]
└─$ sudo tail -f /var/log/syslog | grep "iptables-input"
[sudo] password for kali:
```

****
****

63. Delete the command history.

```
┌──(kali㉿kali)-[~]
└─$ history -c
```

_This clears the current shell's history. To ensure it's also removed from the history file:

```
┌──(kali㉿kali)-[~]
└─$ rm ~/.bash_history
```

###63. حذف سجل الأوامر.

```
┌──(kali㉿kali)-[~]
└─$ history -c
```

_هذا يمسح سجل الجلسة الحالية. لضمان إزالته أيضًا من ملف السجل:

```
┌──(kali㉿kali)-[~]
└─$ rm ~/.bash_history
```

****
****

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

###64. البحث عن كلمة "kali" في ملف `/etc/passwd`.

```
┌──(kali㉿kali)-[~]
└─$ grep kali /etc/passwd
kali:x:1000:1000:kali,,,:/home/kali:/usr/bin/zsh
```

This will display any lines in the file that contain the word "kali".

"kali". سيعرض هذا أي سطور في الملف تحتوي على كلمة

****
****

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

###65.**`/etc/group`** في ملف **"kali"** البحث عن كلمة.

```
┌──(kali㉿kali)-[~]
└─$ grep kali /etc/group
adm:x:4:kali
dialout:x:20:kali
cdrom:x:24:kali
floppy:x:25:kali
sudo:x:27:kali
audio:x:29:pulse,kali
dip:x:30:kali
video:x:44:kali
plugdev:x:46:kali
netdev:x:109:kali
wireshark:x:119:kali
bluetooth:x:121:kali
lpadmin:x:126:kali
kali-trusted:x:128:
scanner:x:139:saned,kali
kali:x:1000:
kaboxer:x:144:kali
```

This will show any groups that include **"kali"**.

"kali" سيظهر هذا أي مجموعات تتضمن.

****
****

66. Locate the `passwd` file.

###66.`passwd` العثور على ملف.

```
┌──(kali㉿kali)-[~]
└─$ locate passwd
/etc/passwd
/etc/passwd-
/etc/alternatives/vncpasswd
/etc/alternatives/vncpasswd.1.gz
/etc/pam.d/chpasswd
/etc/pam.d/passwd
/etc/security/opasswd
/usr/bin/autopasswd
/usr/bin/expect_autopasswd
/usr/bin/expect_mkpasswd
/usr/bin/expect_tkpasswd
/usr/bin/gpasswd
/usr/bin/grub-mkpasswd-pbkdf2
/usr/bin/htpasswd
/usr/bin/impacket-smbpasswd
/usr/bin/ldappasswd
/usr/bin/mkpasswd
/usr/bin/passwd
/usr/bin/smbpasswd
```

_Alternatively, you can check its standard location:

_يمكنن التحقق من موقعه القياسي:

```
┌──(kali㉿kali)-[~]
└─$ cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:103:110:MySQL Server,,,:/nonexistent:/bin/false
```

****
****

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

###67.وفتحه **shadow** العثور على ملف.

_The shadow file is usually located at **`/etc/shadow`**. To open it:

_لفتحه . **`/etc/shadow`** موجودًا في **shadow** عادةً ما يكون ملف:

```
┌──(kali㉿kali)-[~]
└─$ sudo cat /etc/shadow
root:!:19989:0:99999:7:::
daemon:*:19989:0:99999:7:::
bin:*:19989:0:99999:7:::
sys:*:19989:0:99999:7:::
sync:*:19989:0:99999:7:::
games:*:19989:0:99999:7:::
man:*:19989:0:99999:7:::
lp:*:19989:0:99999:7:::
mail:*:19989:0:99999:7:::
news:*:19989:0:99999:7:::
uucp:*:19989:0:99999:7:::
```

****
****

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

###68.**`/etc`** البحث عن جميع ملفات التكوين في دليل.

```
┌──(kali㉿kali)-[~]
└─$ find /etc -type f -name "*.conf"
/etc/kismet/kismet.conf
/etc/kismet/kismet_80211.conf
/etc/kismet/kismet_logging.conf
/etc/kismet/kismet_alerts.conf
/etc/kismet/kismet_filter.conf
/etc/kismet/kismet_httpd.conf
/etc/kismet/kismet_memory.conf
/etc/kismet/kismet_uav.conf
```

_This command finds all files with the **`.conf`** extension.

_**`.conf`** هذا الأمر يبحث عن جميع الملفات ذات الامتداد.

****
****

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

###69. البحث بشكل متكرر عن كلمة محددة في دليل **`/var/log`**.

```
┌──(kali㉿kali)-[~]
└─$ grep -r "kawther" /var/log
grep: /var/log/vmware-vmsvc-root.log: Permission denied
grep: /var/log/vmware-vmsvc-root.1.log: Permission denied
grep: /var/log/private: Permission denied
grep: /var/log/lightdm: Permission denied
grep: /var/log/vmware-vmtoolsd-root.log: Permission denied
grep: /var/log/boot.log.1: Permission denied
grep: /var/log/btmp: Permission denied
grep: /var/log/boot.log: Permission denied
grep: /var/log/speech-dispatcher: Permission denied
grep: /var/log/installer/Xorg.0.log: Permission denied
grep: /var/log/installer/partman: Permission denied
grep: /var/log/installer/syslog: Permission denied
grep: /var/log/installer/cdebconf/templates.dat: Permission denied
grep: /var/log/installer/cdebconf/questions.dat: Permission denied
/var/log/auth.log:Sep 24 18:38:03 kali sudo:     kali : TTY=pts/0 ; PWD=/home/kali/Desktop ; USER=root ; COMMAND=/usr/sbin/adduser kawther
/var/log/auth.log:Sep 24 18:38:03 kali groupadd[35060]: group added to /etc/group: name=kawther, GID=1001
/var/log/auth.log:Sep 24 18:38:03 kali groupadd[35060]: group added to /etc/gshadow: name=kawther
/var/log/auth.log:Sep 24 18:38:03 kali groupadd[35060]: new group: name=kawther, GID=1001
/var/log/auth.log:Sep 24 18:38:03 kali useradd[35066]: new user: name=kawther, UID=1001, GID=1001, home=/home/kawther, shell=/bin/bash, from
/var/log/auth.log:Sep 24 18:38:25 kali passwd[35075]: pam_unix(passwd:chauthtok): password changed for kawther
/var/log/auth.log:Sep 24 18:39:32 kali chfn[35160]: changed user 'kawther' information
/var/log/auth.log:Sep 24 18:43:41 kali sudo:     kali : TTY=pts/0 ; PWD=/home/kali/Desktop ; USER=root ; COMMAND=/usr/bin/passwd kawther
/var/log/auth.log:Sep 24 18:44:14 kali passwd[36534]: pam_unix(passwd:chauthtok): password changed for kawther
/var/log/auth.log:Sep 24 18:55:18 kali sudo:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/sbin/usermod -aG sudo kawther
/var/log/auth.log:Sep 24 18:55:18 kali usermod[39797]: add 'kawther' to group 'sudo'
```

****
****

70. View the system's kernel version.

###70.عرض إصدار نواة النظام لديك.

```
┌──(kali㉿kali)-[~]
└─$ uname -r
5.18.0-kali5-amd64
```

Or:

```
┌──(kali㉿kali)-[~]
└─$ uname -a
Linux kali 5.18.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 5.18.5-1kali6 (2022-07-07) x86_64 GNU/Linux
```

_معلومات إضافية مثل اسم النظام ونوع المعيار.

****
****

71. Display the system's memory usage.

###71.عرض استخدام الذاكرة في النظام.

```
┌──(kali㉿kali)-[~]
└─$ free -h
               total        used        free      shared  buff/cache   available
Mem:           1.9Gi       895Mi       262Mi        29Mi       789Mi       830Mi
Swap:          974Mi       289Mi       685Mi
```

_This command shows the total, used, and available memory in a human-readable format.

_هذا الأمر يعرض الذاكرة الكلية والمستخدمة والمتاحة بشكل قابل للقراءة.

****
****

72. Show the system's disk usage.

###72.عرض استخدام القرص في النظام.

```
┌──(kali㉿kali)-[~]
└─$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            939M     0  939M   0% /dev
tmpfs           195M  1.3M  194M   1% /run
/dev/sda1        48G   13G   33G  29% /
tmpfs           974M     0  974M   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           195M  140K  195M   1% /run/user/1000
tmpfs           195M  4.0K  195M   1% /run/user/127
```

_This command displays the file system disk space usage in a human-readable format.

_هذا الأمر يعرض استخدام مساحة القرص في نظام الملفات بشكل قابل للقراءة.

****
****

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

###73. تحقق من زمن التشغيل ومتوسط الحمل في النظام.

```
┌──(kali㉿kali)-[~]
└─$ uptime
 08:07:42 up 16:21,  1 user,  load average: 0.06, 0.36, 0.39
```

_This command shows how long the system has been running and the current load averages.

_هذا الأمر يعرض مدة تشغيل النظام ومتوسط الأحمال الحالية.

****
****

74. Display the current logged-in users.

###74.عرض المستخدمين المسجلين حاليًا.

```
┌──(kali㉿kali)-[~]
└─$ who
kali     tty7         2024-09-24 15:23 (:0)
```

_هذا الأمر يعرض جميع المستخدمين المسجلين حاليًا في النظام.

****
****

75. Check the identity of the current user.

###75. تحقق من هوية المستخدم الحالي.

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

_This command returns the username of the current user.

_هذا الأمر يعيد اسم المستخدم الحالي.

****
****

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

```
┌──(kali㉿kali)-[~]
└─$ sudo cat /var/log/auth.log
[sudo] password for kali:
Sep 23 17:29:04 kali systemd-logind[533]: New seat seat0.
Sep 23 17:29:04 kali systemd-logind[533]: Watching system buttons on /dev/input/event1 (Power Button)
Sep 23 17:29:04 kali systemd-logind[533]: Watching system buttons on /dev/input/event0 (AT Translated Set 2 keyboard)
Sep 23 17:29:05 kali lightdm: pam_unix(lightdm-greeter:session): session opened for user lightdm(uid=127) by (uid=0)
Sep 23 17:29:05 kali systemd-logind[533]: New session c1 of user lightdm.
Sep 23 17:29:05 kali systemd: pam_unix(systemd-user:session): session opened for user lightdm(uid=127) by (uid=0)
Sep 23 17:29:20 kali lightdm: pam_unix(lightdm-greeter:session): session closed for user lightdm
Sep 23 17:29:20 kali lightdm: pam_unix(lightdm:session): session opened for user kali(uid=1000) by (uid=0)
Sep 23 17:29:20 kali systemd-logind[533]: Removed session c1.
Sep 23 17:29:20 kali systemd-logind[533]: New session 2 of user kali.
Sep 23 17:29:20 kali systemd: pam_unix(systemd-user:session): session opened for user kali(uid=1000) by (uid=0)
Sep 23 17:29:48 kali polkitd(authority=local): Registered Authentication Agent for unix-session:2 (system bus name :1.
/lib/policykit-1-gnome/polkit-gnome-authentication-agent-1], object path /org/gnome/PolicyKit1/AuthenticationAgent, lo
```

_You may also use `less` or `tail` for easier navigation:

```
┌──(kali㉿kali)-[~]
└─$ sudo less /var/log/auth.log

zsh: suspended  sudo less /var/log/auth.log
```

###76. عرض ملف `/var/log/auth.log`.

```
┌──(kali㉿kali)-[~]
└─$ sudo cat /var/log/auth.log
[sudo] password for kali:
Sep 23 17:29:04 kali systemd-logind[533]: New seat seat0.
Sep 23 17:29:04 kali systemd-logind[533]: Watching system buttons on /dev/input/event1 (Power Button)
Sep 23 17:29:04 kali systemd-logind[533]: Watching system buttons on /dev/input/event0 (AT Translated Set 2 keyboard)
Sep 23 17:29:05 kali lightdm: pam_unix(lightdm-greeter:session): session opened for user lightdm(uid=127) by (uid=0)
Sep 23 17:29:05 kali systemd-logind[533]: New session c1 of user lightdm.
Sep 23 17:29:05 kali systemd: pam_unix(systemd-user:session): session opened for user lightdm(uid=127) by (uid=0)
Sep 23 17:29:20 kali lightdm: pam_unix(lightdm-greeter:session): session closed for user lightdm
Sep 23 17:29:20 kali lightdm: pam_unix(lightdm:session): session opened for user kali(uid=1000) by (uid=0)
Sep 23 17:29:20 kali systemd-logind[533]: Removed session c1.
Sep 23 17:29:20 kali systemd-logind[533]: New session 2 of user kali.
Sep 23 17:29:20 kali systemd: pam_unix(systemd-user:session): session opened for user kali(uid=1000) by (uid=0)
Sep 23 17:29:48 kali polkitd(authority=local): Registered Authentication Agent for unix-session:2 (system bus name :1.
/lib/policykit-1-gnome/polkit-gnome-authentication-agent-1], object path /org/gnome/PolicyKit1/AuthenticationAgent, lo
```

_لتسهيل التنقل `tail` أو `less` يمكنك أيضًا استخدام.

```
┌──(kali㉿kali)-[~]
└─$ sudo less /var/log/auth.log

zsh: suspended  sudo less /var/log/auth.log
```

****
****

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

###77. بشكل آمن `auth.log` حذف ملف.

```
┌──(kali㉿kali)-[~]
└─$ sudo shred -u /var/log/auth.log
```

_This command overwrites the file to make recovery difficult before deleting it.

_هذا الأمر يكتب فوق الملف لجعل استعادته صعبًا قبل حذفه.

****
****

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

###78. كيف يمكنك قفل حساب مستخدم لمنعهم من تسجيل الدخول.

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

****
****

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

###79. ما هو الأمر الذي يمكنك استخدامه لتغيير قشرة المستخدم الافتراضية.

```
┌──(kali㉿kali)-[~]
└─$ sudo chsh -s /bin/zsh  kawther
```

****
****

80. Display the system's boot messages.

###80.عرض رسائل بدء تشغيل النظام.

```
┌──(kali㉿kali)-[~]
└─$ sudo dmesg
[sudo] password for kali:
[    0.000000] Linux version 5.18.0-kali5-amd64 (devel@kali.org) (gcc-11 (Debian 11.3.0-3) 11.3.0, GNU ld (GNU Binutils for Debian) 2
.38) #1 SMP PREEMPT_DYNAMIC Debian 5.18.5-1kali6 (2022-07-07)
[    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-5.18.0-kali5-amd64 root=UUID=944e548c-218c-4fbd-9562-f0b63348aa0e ro quiet spla
sh
[    0.000000] Disabled fast string operations
[    0.000000] x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
[    0.000000] x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
[    0.000000] x86/fpu: xstate_offset[2]:  576, xstate_sizes[2]:  256
[    0.000000] x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using 'compacted' format.
[    0.000000] signal: max sigframe size: 1776
[    0.000000] BIOS-provided physical RAM map:
[    0.000000] BIOS-e820: [mem 0x0000000000000000-0x000000000009ebff] usable
[    0.000000] BIOS-e820: [mem 0x000000000009ec00-0x000000000009ffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000000dc000-0x00000000000fffff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000000100000-0x000000007fedffff] usable
[    0.000000] BIOS-e820: [mem 0x000000007fee0000-0x000000007fefefff] ACPI data
[    0.000000] BIOS-e820: [mem 0x000000007feff000-0x000000007fefffff] ACPI NVS
[    0.000000] BIOS-e820: [mem 0x000000007ff00000-0x000000007fffffff] usable
[    0.000000] BIOS-e820: [mem 0x00000000f0000000-0x00000000f7ffffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000fec00000-0x00000000fec0ffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000fffe0000-0x00000000ffffffff] reserved
[    0.000000] NX (Execute Disable) protection: active
[    0.000000] SMBIOS 2.7 present.
```

**********انتهابحمدالله**********

أعداد الطالبة: كوثر توفيق يحيى الدغار.