Department\Cyber Security

Group\ Second

Eng. Ghadeer Alamadhagi

الجمهورية اليمنية

وزارة التعليم العالي والبحث العلمي

جامعـــــة الـــــــــــــرازي

كليه الحاسوب وتقنيه المعلومات

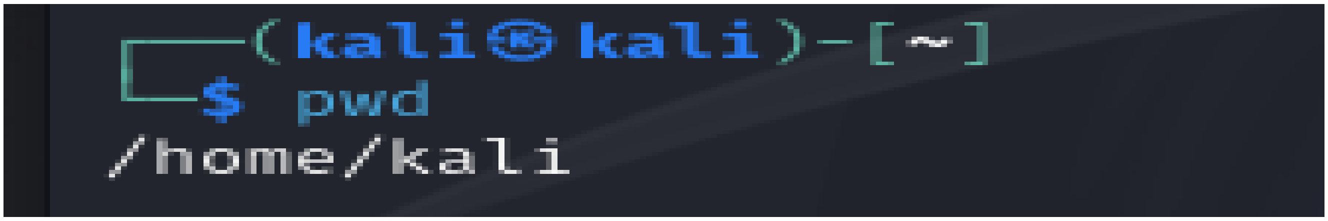
بسم الله الرحمن الرحيم

SOME KALI LINUX COMMANDS

Section 1: File and Directory Management

1. Display the current working directory.

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

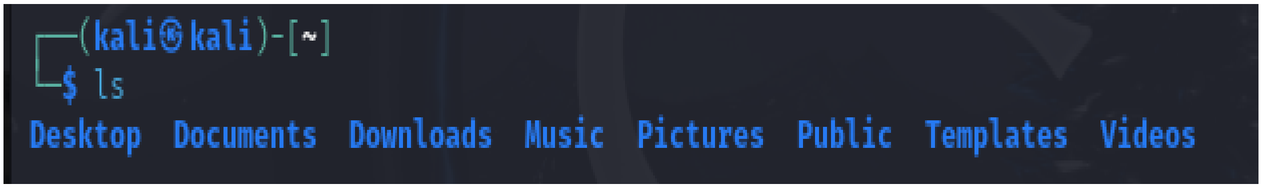


```
┌──(kali㉿kali)-[~]
└─$ pwd
/home/kali
```

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

يعرض جميع الملفات والمجلدات في الدليل الحالي، بما في ذلك الملفات الخفيه

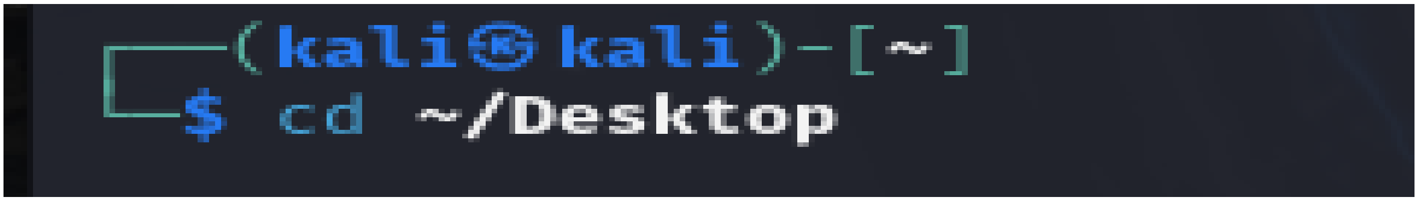
يساعد في معرفة محتويات المجلد



```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
```

3- Change your directory to the `Desktop`

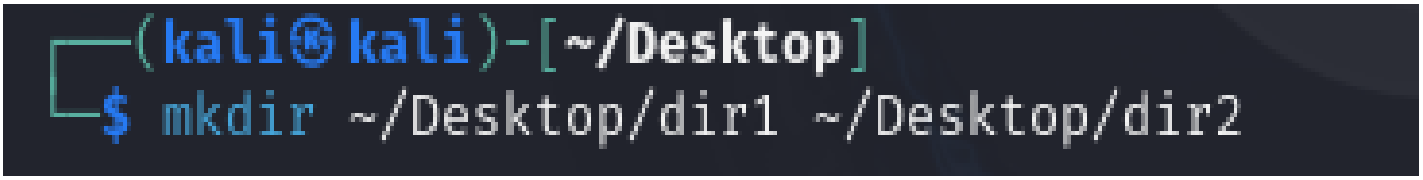
يُستخدم لتغيير الدليل الحالي إلى دليل آخر. في هذا المثال، ينتقل إلى مجلد سطح المكتب .



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

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

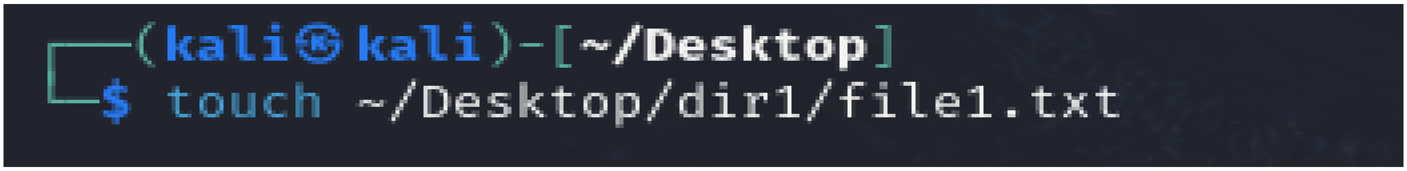
`dir2 `و `dir1 يُستخدم لإنشاء مجلدات جديدة. في هذا المثال، ينشئ مجلدين باسم.



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

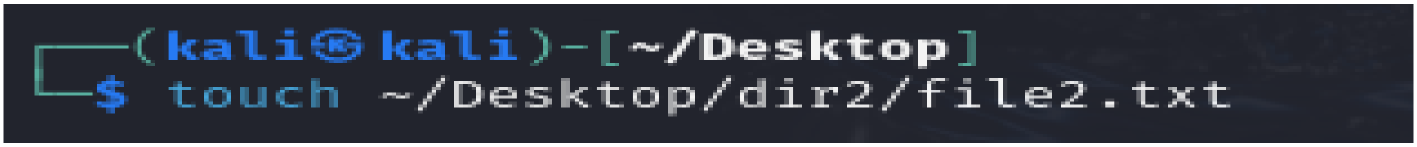
5. Inside `dir1`, create a file named `file1.txt`

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



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

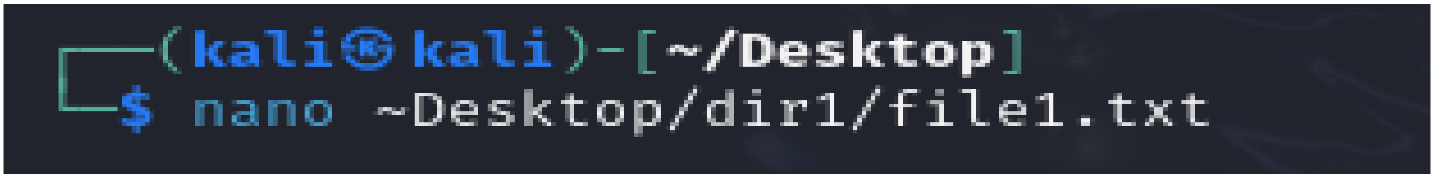
6. Inside `dir2`, create a file named `file2.txt`.



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

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

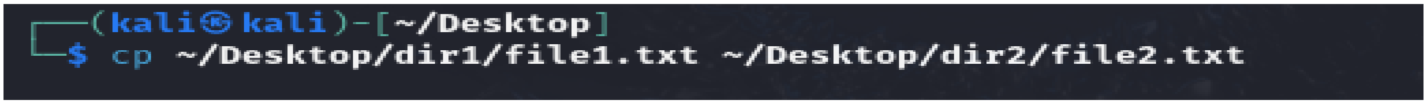
محررات نصوص تُستخدم لتحرير الملفات النصية من خالل واجهة سطر الأوامر



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

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

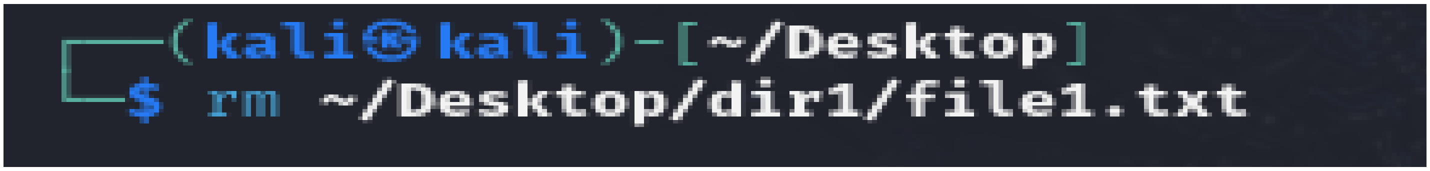
يُستخدم لنسخ الملفات أو المجلدات من موقع إلى آخر. هنا، ينقل محتويات ملف إلى ملف آخر



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

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

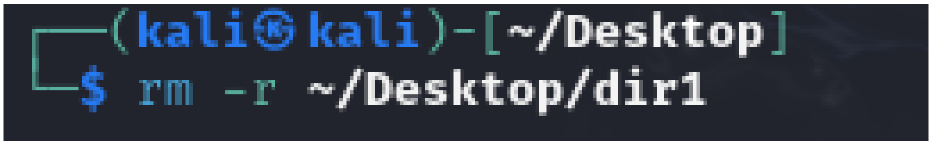
يُستخدم لحذف الملفات. في هذا المثال، يقوم بحذف ملف معين .



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

10. Remove the directory `dir1` from the Desktop

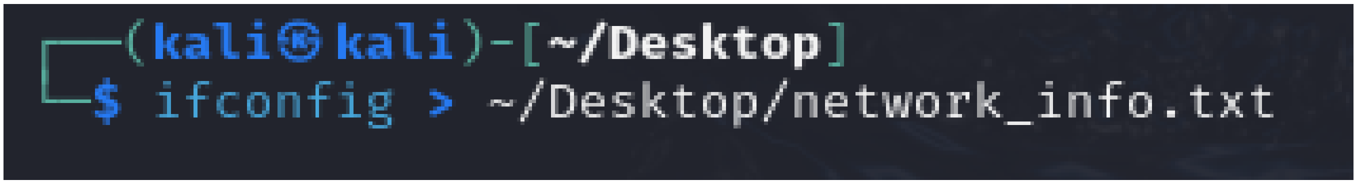
يُستخدم لحذف مجلد فارغ .



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

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

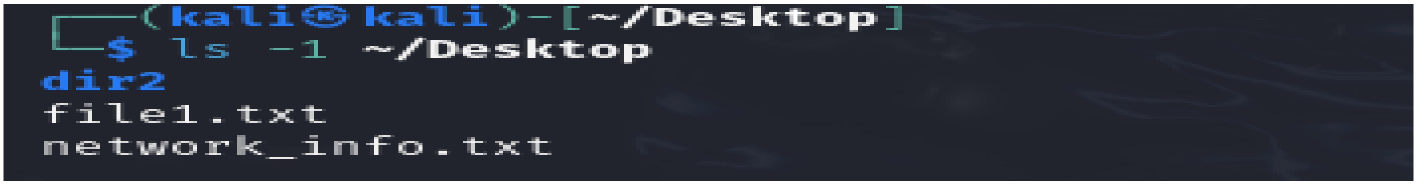
من عرضها على الشاشة. يُستخدم `ifconfig إلى ملف بدلاً يقوم بتوجيه مخرجات أمر
لحفظ معلومات الشبكة في ملف.



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

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

◌ُ◌ُ يستخدم لعرض ملفات المجلد الحالي مع جميع التفاصيل مثل ألأذونات، المالك، وحجم الملف.

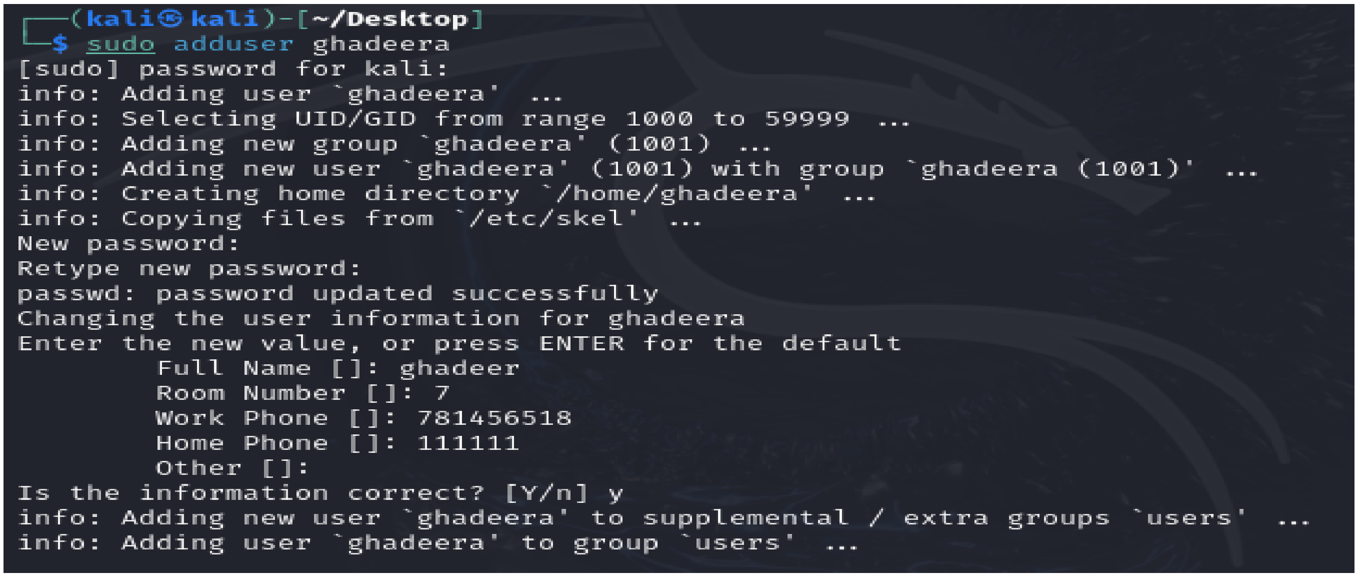


```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls -1 ~/Desktop
dir2
file1.txt
network_info.txt
```

Section 2: Users and Groups Management

13. Create a new user with your name.

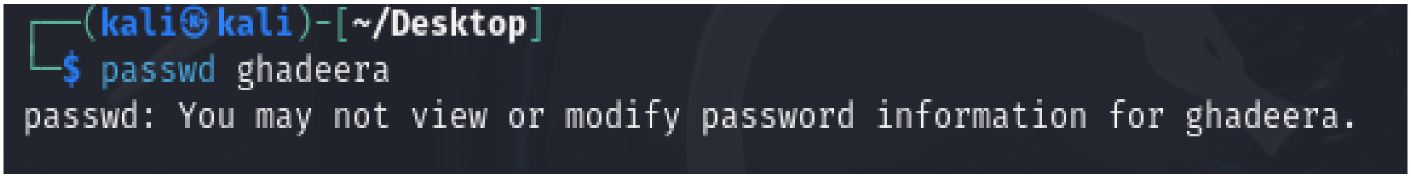
يُستخدم لإنشاء حساب مستخدم جديد على النظام



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo adduser ghadeera
[sudo] password for kali:
info: Adding user `ghadeera' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `ghadeera' (1001) ...
info: Adding new user `ghadeera' (1001) with group `ghadeera (1001)' ...
info: Creating home directory `/home/ghadeera' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for ghadeera
Enter the new value, or press ENTER for the default
        Full Name []: ghadeer
        Room Number []: 7
        Work Phone []: 781456518
        Home Phone []: 111111
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `ghadeera' to supplemental / extra groups `users' ...
info: Adding user `ghadeera' to group `users' ...
```

14. Set a password for your user.

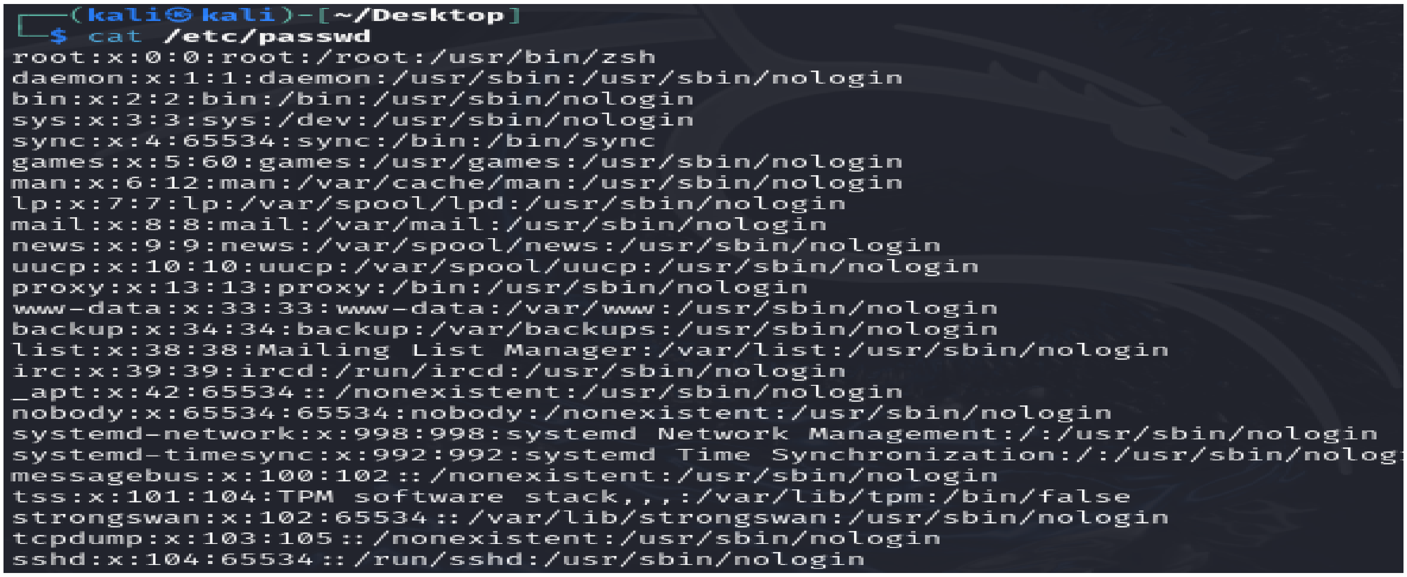
يُستخدم لتعيين أو تغيير كلمة المرور للمستخدم



```
┌──(kali㉿kali)-[~/Desktop]
└─$ passwd ghadeera
passwd: You may not view or modify password information for ghadeera.
```

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

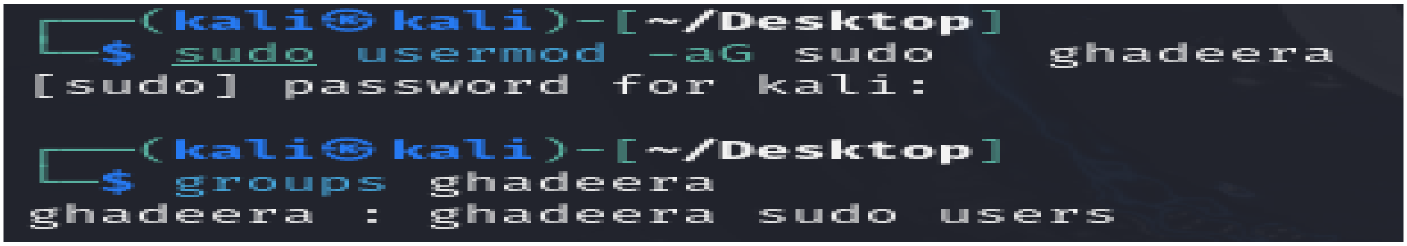
الذي يحتوي على معلومات المستخدمين في النظام. `passwd` يعرض محتويات ملف .



```
┌──(kali㉿kali)-[~/Desktop]
└─$ 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
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:992:992:systemd Time Synchronization:/:/usr/sbin/nolog
messagebus:x:100:102::/nonexistent:/usr/sbin/nologin
tss:x:101:104:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:102:65534::/var/lib/strongswan:/usr/sbin/nologin
tcpdump:x:103:105::/nonexistent:/usr/sbin/nologin
sshd:x:104:65534::/run/sshd:/usr/sbin/nologin
```

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

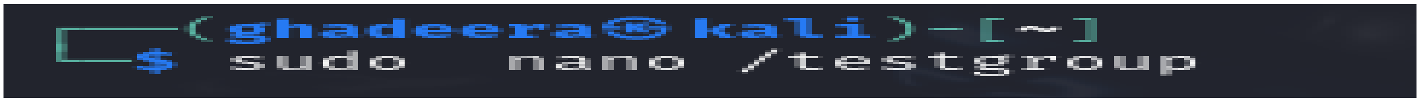
يُستخدم لإضافة مستخدم إلى مجموعة معينة



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

┌──(kali㉿kali)-[~/Desktop]
└─$ groups ghadeera
ghadeera : ghadeera sudo users
```

18. Create a new group named `testgroup`

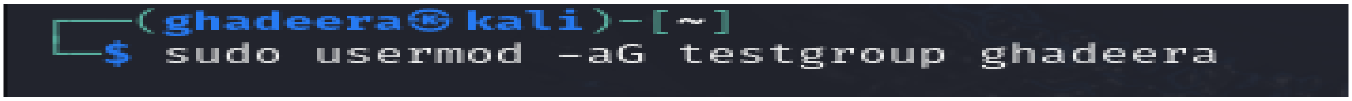
يُستخدم لإنشاء مجموعة جديدة .



```
┌──(ghadeera㉿kali)-[~]
└─$ sudo  nano /testgroup
```

19. Add your user to `testgroup`.

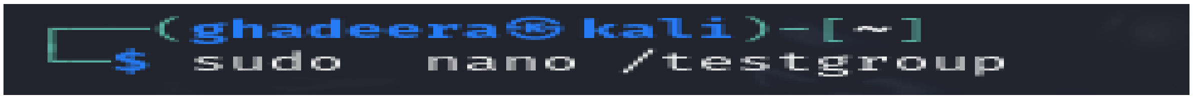
إضافة المستخدم الخاص بي الى "testgroup



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

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

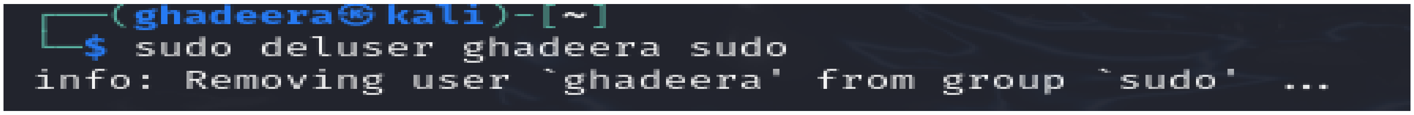
إضافة `testgroup `إلى ملف يعطي صالحيات إدارية:



```
┌──(ghadeera㉿kali)-[~]
└─$ sudo  nano /testgroup
```

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

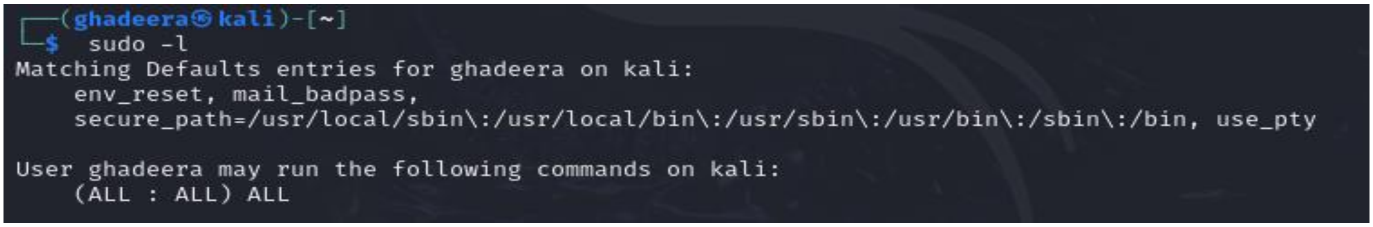
إزالة المستخدم الخاص بك من الملف الذي يعطيه صالحيات إدارية:



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

22. Check if your user still have administrative privileges.

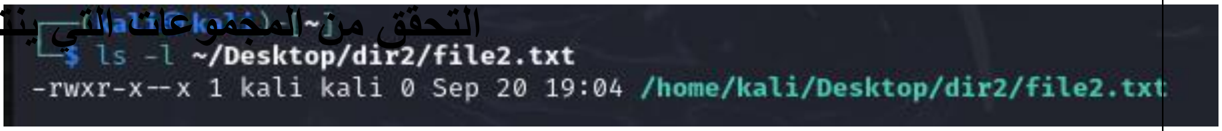
التحقق مما إذا كان المستخدم ال يزال لديه صالحيات إدارية:



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

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

23. Check which groups your user belongs to.

التحقق من المجموعات التي ينتمي إليها المستخدم

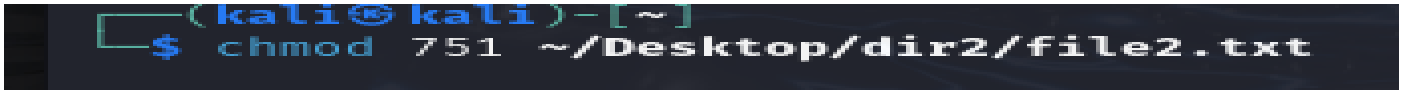


```
┌──(kali㉿kali)-[~]
└─$ ls -l ~/Desktop/dir2/file2.txt
-rwxr-x--x 1 kali kali 0 Sep 20 19:04 /home/kali/Desktop/dir2/file2.txt
```

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 .

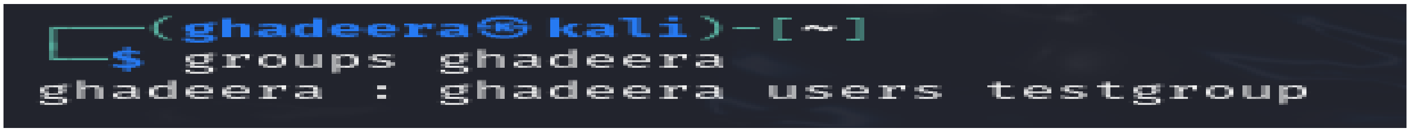
على سطح المكتب `تعيين صالحيات الملف



```
┌──(kali㉿kali)-[~]
└─$ chmod 751 ~/Desktop/dir2/file2.txt
```

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

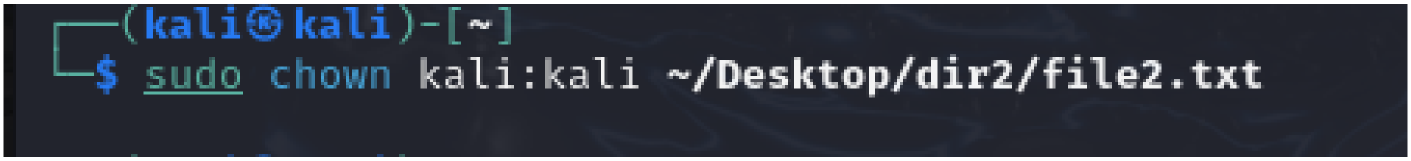
التحقق من صالحيات:



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

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

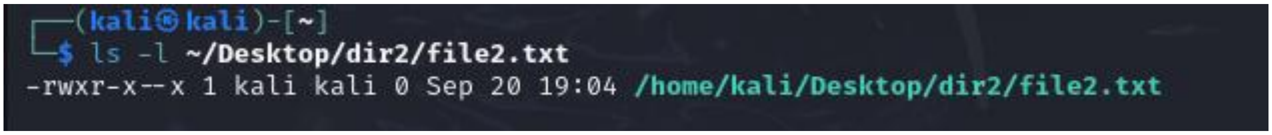
إلى المستخدم الخاص بك` تغيير ملكية



```
┌──(kali㉿kali)-[~]
└─$ sudo chown kali:kali ~/Desktop/dir2/file2.txt
```

27. verify the ownership of `file2.txt`

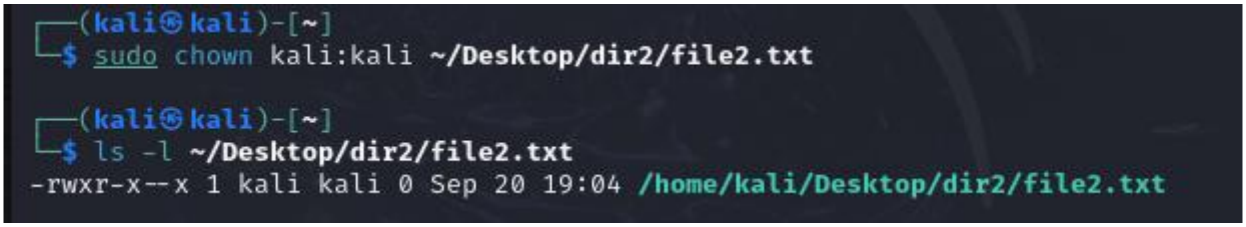
التحقق من ملكية .الملف



```
┌──(kali㉿kali)-[~]
└─$ ls -l ~/Desktop/dir2/file2.txt
-rwxr-x--x 1 kali kali 0 Sep 20 19:04 /home/kali/Desktop/dir2/file2.txt
```

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

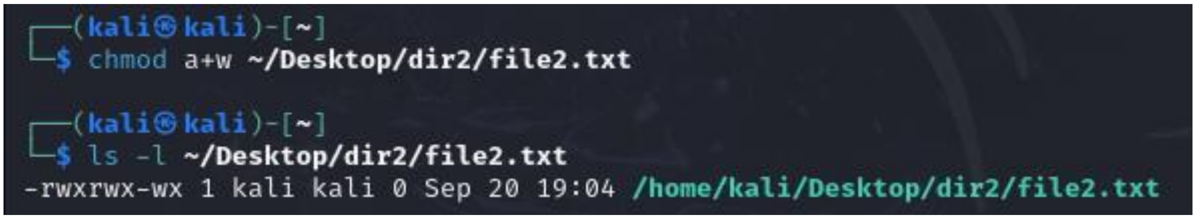
إعادة تغيير ملكية الملف



```
┌──(kali㉿kali)-[~]
└─$ sudo chown kali:kali ~/Desktop/dir2/file2.txt

┌──(kali㉿kali)-[~]
└─$ ls -l ~/Desktop/dir2/file2.txt
-rwxr-x--x 1 kali kali 0 Sep 20 19:04 /home/kali/Desktop/dir2/file2.txt
```

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

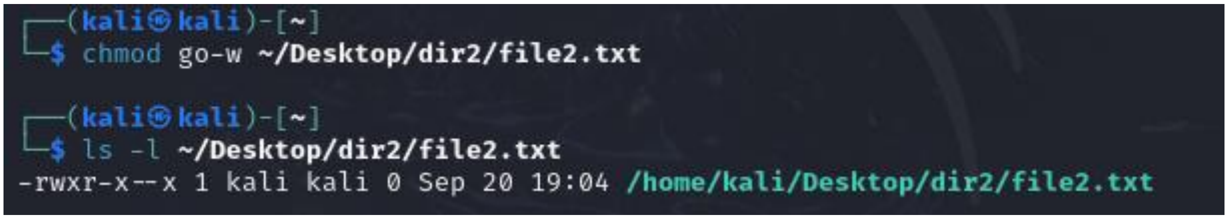
منح الجميع صالحية الكتابة على الملف .



```
┌──(kali㉿kali)-[~]
└─$ chmod a+w ~/Desktop/dir2/file2.txt

┌──(kali㉿kali)-[~]
└─$ ls -l ~/Desktop/dir2/file2.txt
-rwxrwx-wx 1 kali kali 0 Sep 20 19:04 /home/kali/Desktop/dir2/file2.txt
```

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

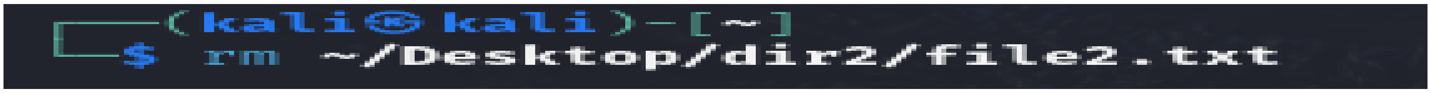
:إزالة صالحية الكتابة للمجموعة واآلخرين .



```
┌──(kali㉿kali)-[~]
└─$ chmod go-w ~/Desktop/dir2/file2.txt

┌──(kali㉿kali)-[~]
└─$ ls -l ~/Desktop/dir2/file2.txt
-rwxr-x--x 1 kali kali 0 Sep 20 19:04 /home/kali/Desktop/dir2/file2.txt
```

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

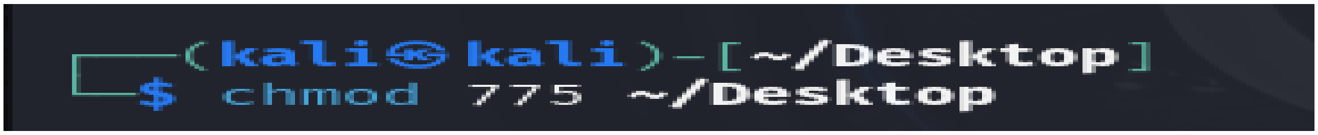
بعد: تغيير الملكية والصالحيات الضرورية` ` حذف .



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

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

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

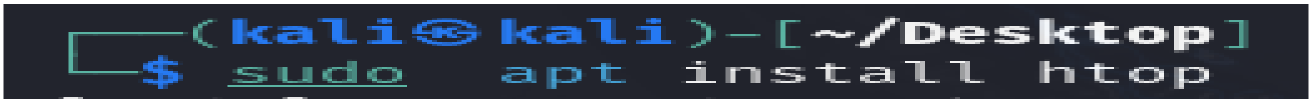


```
┌──(kali㉿kali)-[~/Desktop]
└─$ chmod 775 ~/Desktop
```

Section 4: Process Management

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

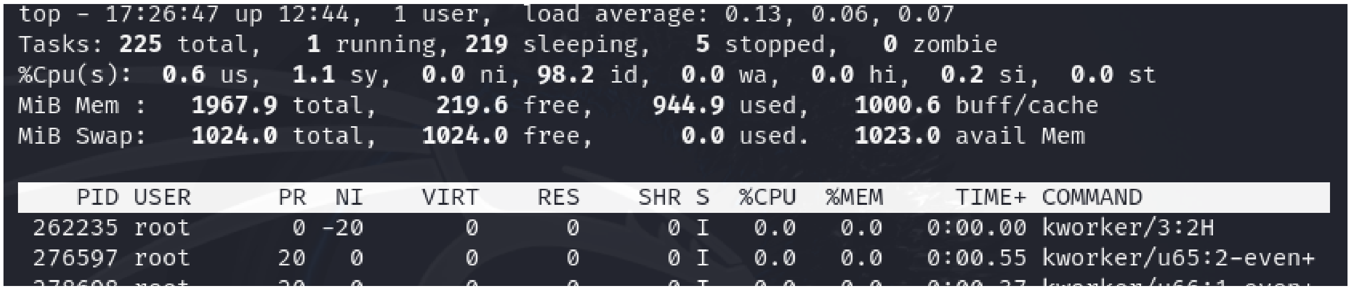
`htop تثبيت أداة مراقبة العمليات .



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo apt install htop
```

34. Display all running processes.

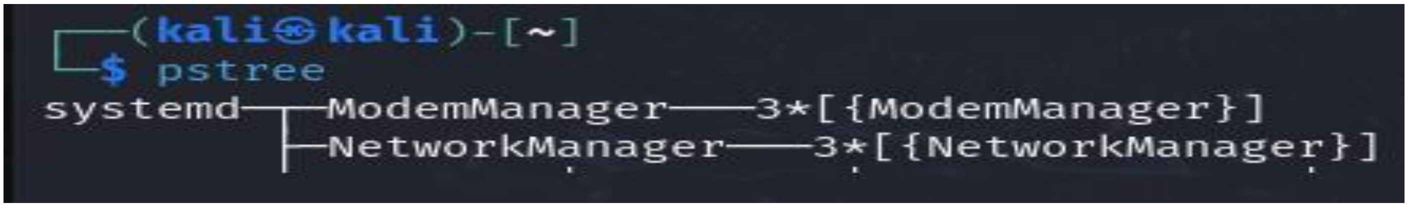
عرض جميع العمليات الجارية:



```
top - 17:26:47 up 12:44,  1 user,  load average: 0.13, 0.06, 0.07
Tasks: 225 total,   1 running, 219 sleeping,   5 stopped,   0 zombie
%Cpu(s):  0.6 us,  1.1 sy,  0.0 ni, 98.2 id,  0.0 wa,  0.0 hi,  0.2 si,  0.0 st
MiB Mem :   1967.9 total,    219.6 free,    944.9 used,   1000.6 buff/cache
MiB Swap:   1024.0 total,   1024.0 free,      0.0 used.   1023.0 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
 262235 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/3:2H
 276597 root      20   0       0      0      0 I   0.0   0.0   0:00.55 kworker/u65:2-even+
 278698 root      20   0       0      0      0 I   0.0   0.0   0:00.37 kworker/u66:1-even+
```

35. Display a tree of all running processes.

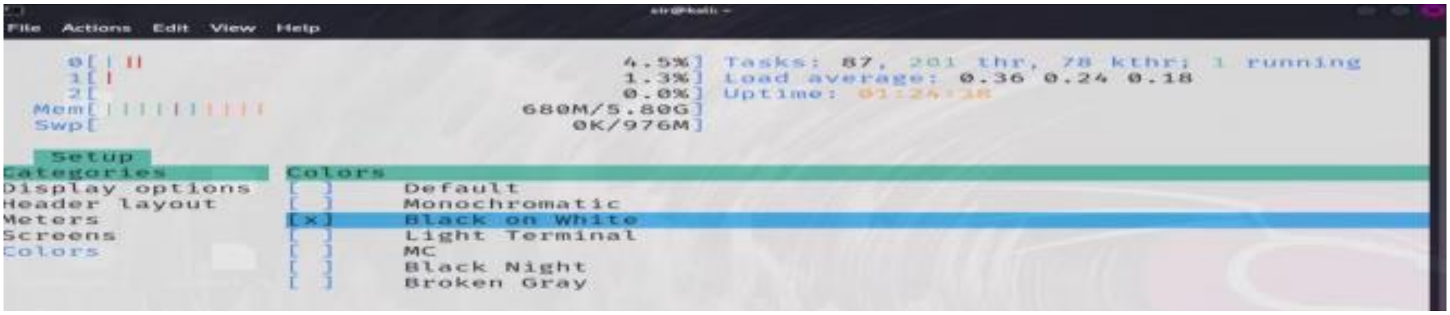
عرض شجرة العمليات الجارية



```
┌──(kali㉿kali)-[~]
└─$ pstree
systemd─┬─ModemManager───3*[{ModemManager}]
        ├─NetworkManager───3*[{NetworkManager}]
```

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

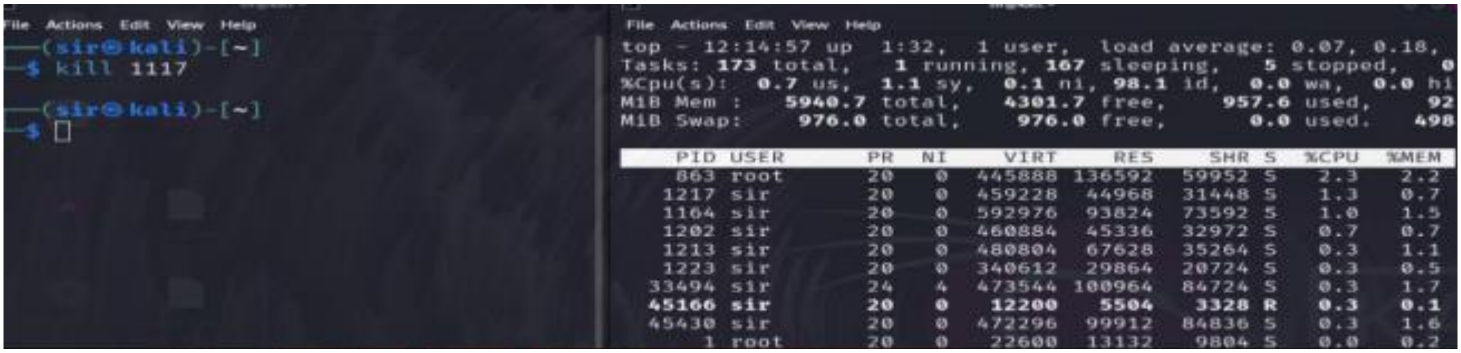
: PID فتح عارض العمليات التفاعلي وتحديد عملية بناًء على .



```
    0[| ||                                 4.5%]  Tasks: 87, 201 thr, 78 kthr; 1 running
    1[|                                    1.3%]  Load average: 0.36 0.24 0.18
    2[                                     0.0%]  Uptime: 01:24:38
  Mem[||||||||||||                   680M/5.80G]
  Swp[                                  0K/976M]

   Setup
Categories          Colors
Display options     [ ]      Default
Header layout       [ ]      Monochromatic
Meters              [x]      Black on White
Screens             [ ]      Light Terminal
Colors              [ ]      MC
                    [ ]      Black Night
                    [ ]      Broken Gray
```

37. Kill a process with a specific PID

PID قتل عملية معينة باستخدام .

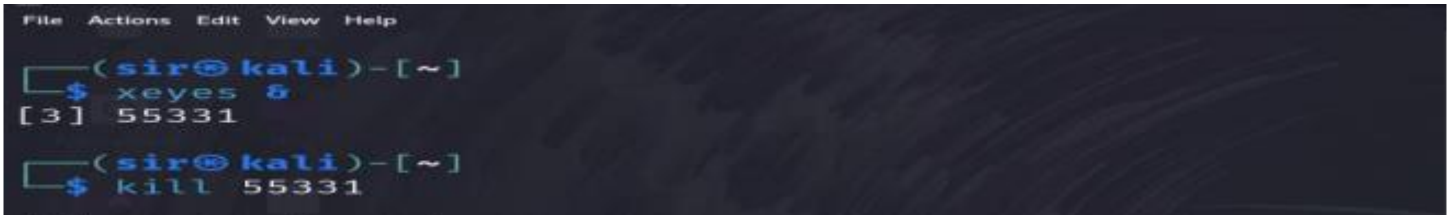


```
┌──(sir㉿kali)-[~]
└─$ kill 1117

┌──(sir㉿kali)-[~]
└─$ ▯
```

```
top - 12:14:57 up  1:32,  1 user,  load average: 0.07, 0.18,
Tasks: 173 total,   1 running, 167 sleeping,   5 stopped,   0
%Cpu(s):  0.7 us,  1.1 sy,  0.1 ni, 98.1 id,  0.0 wa,  0.0 hi
MiB Mem :   5940.7 total,   4301.7 free,    957.6 used,    92
MiB Swap:    976.0 total,    976.0 free,      0.0 used.   498

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM
    863 root      20   0  445888 136592  59952 S   2.3   2.2
   1217 sir       20   0  459228  44968  31448 S   1.3   0.7
   1164 sir       20   0  592976  93824  73592 S   1.0   1.5
   1202 sir       20   0  460884  45336  32972 S   0.7   0.7
   1213 sir       20   0  480804  67628  35264 S   0.3   1.1
   1223 sir       20   0  340612  29864  20724 S   0.3   0.5
  33494 sir       24   4  473544 100964  84724 S   0.3   1.7
  45166 sir       20   0   12200   5504   3328 R   0.3   0.1
  45430 sir       20   0  472296  99912  84836 S   0.3   1.6
      1 root      20   0   22600  13132   9804 S   0.0   0.2
```

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

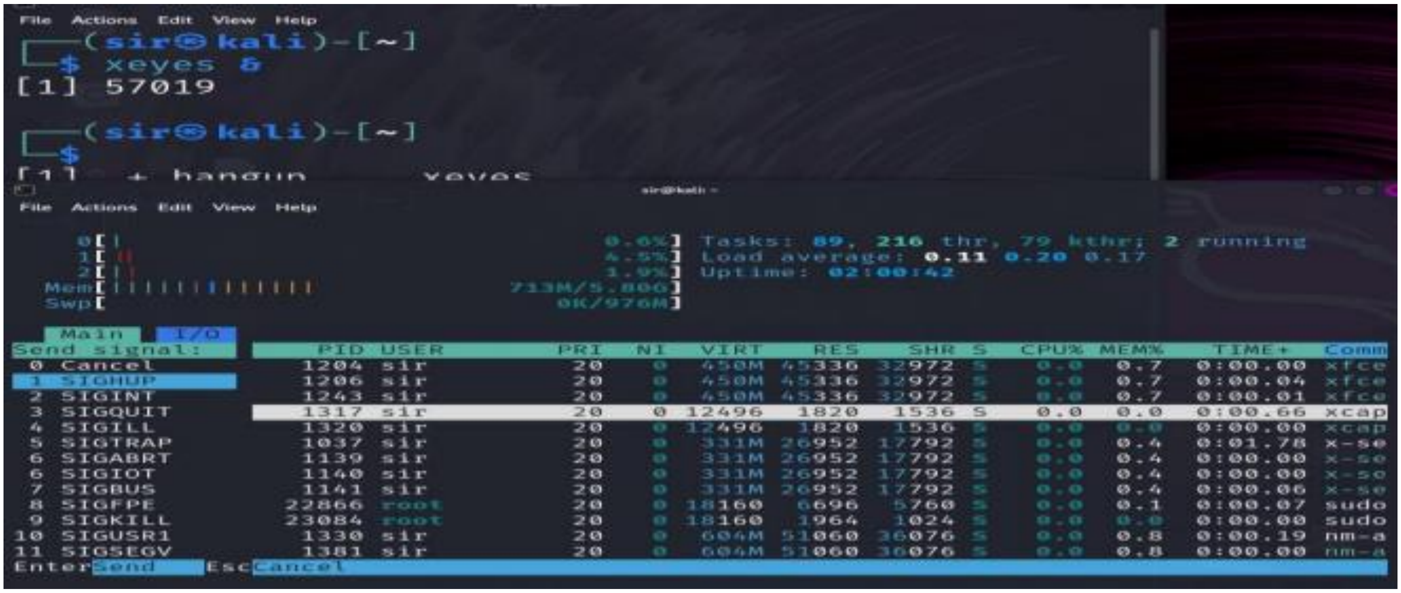
exeyes) بدء تطبيق وإيقافه باستخدام أمر يقتل العمليات باالسم



```
┌──(sir㉿kali)-[~]
└─$ xeyes &
[3] 55331

┌──(sir㉿kali)-[~]
└─$ kill 55331
```

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

إعادة تشغيل التطبيق، ثم إيقافه باستخدام عارض العمليات التفاعلي:

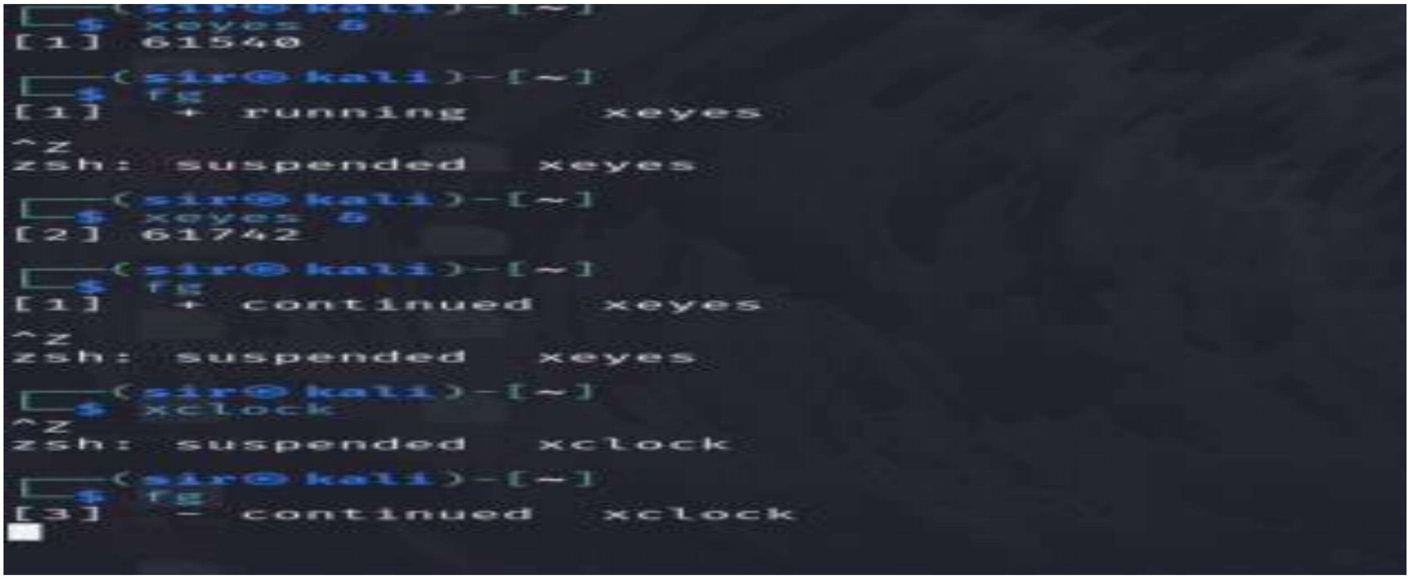


```
┌──(sir㉿kali)-[~]
└─$ xeyes &
[1] 57019

┌──(sir㉿kali)-[~]
└─$
[1]  + hangup      xeyes
```

```
    0[|                                  0.6%]   Tasks: 89, 216 thr, 79 kthr; 2 running
    1[||                                 4.5%]   Load average: 0.11 0.20 0.17
    2[||                                 1.9%]   Uptime: 02:00:42
  Mem[||||||||||||||||           713M/5.80G]
  Swp[                              0K/976M]

  Main   I/O
Send signal:      PID USER      PRI  NI  VIRT   RES   SHR S  CPU% MEM%   TIME+  Comm
 0 Cancel        1204 sir        20   0  450M 45336 32972 S   0.0  0.7  0:00.00 xfce
 1 SIGHUP        1206 sir        20   0  450M 45336 32972 S   0.0  0.7  0:00.04 xfce
 2 SIGINT        1243 sir        20   0  450M 45336 32972 S   0.0  0.7  0:00.01 xfce
 3 SIGQUIT       1317 sir        20   0 12496  1820  1536 S   0.0  0.0  0:00.66 xcap
 4 SIGILL        1320 sir        20   0 12496  1820  1536 S   0.0  0.0  0:00.00 xcap
 5 SIGTRAP       1037 sir        20   0  331M 26952 17792 S   0.0  0.4  0:01.78 x-se
 6 SIGABRT       1139 sir        20   0  331M 26952 17792 S   0.0  0.4  0:00.00 x-se
 6 SIGIOT        1140 sir        20   0  331M 26952 17792 S   0.0  0.4  0:00.00 x-se
 7 SIGBUS        1141 sir        20   0  331M 26952 17792 S   0.0  0.4  0:00.06 x-se
 8 SIGFPE       22866 root       20   0 18160  6696  5760 S   0.0  0.1  0:00.07 sudo
 9 SIGKILL      23084 root       20   0 18160  1964  1024 S   0.0  0.0  0:00.00 sudo
10 SIGUSR1       1330 sir        20   0  604M 51060 36076 S   0.0  0.8  0:00.19 nm-a
11 SIGSEGV       1381 sir        20   0  604M 51060 36076 S   0.0  0.8  0:00.00 nm-a
EnterSend      EscCancel
```

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

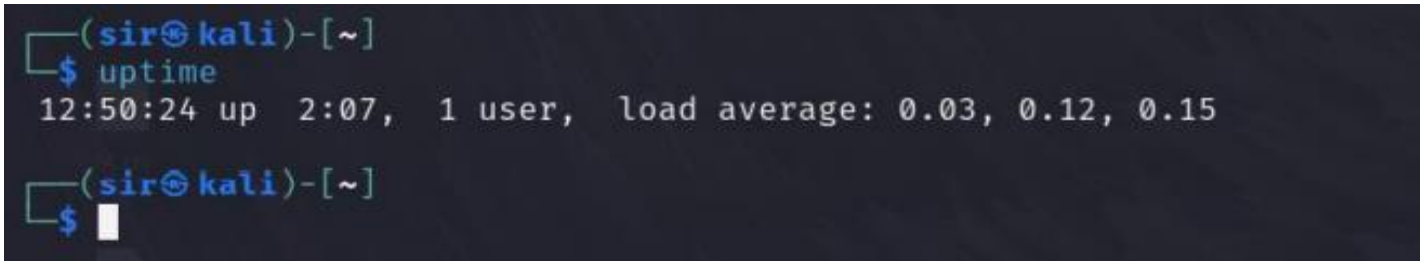
تشغيل أمر في الخلفية، ثم إحضاره إلى المقدمة)exeyes :)



```
┌──(sir㉿kali)-[~]
└─$ xeyes &
[1] 61540

┌──(sir㉿kali)-[~]
└─$ fg
[1]  + running    xeyes
^Z
zsh: suspended  xeyes

┌──(sir㉿kali)-[~]
└─$ xeyes &
[2] 61742

┌──(sir㉿kali)-[~]
└─$ fg
[1]  + continued  xeyes
^Z
zsh: suspended  xeyes

┌──(sir㉿kali)-[~]
└─$ xclock
^Z
zsh: suspended  xclock

┌──(sir㉿kali)-[~]
└─$ fg
[3]  - continued  xclock
```

41. Check how long the system has been running

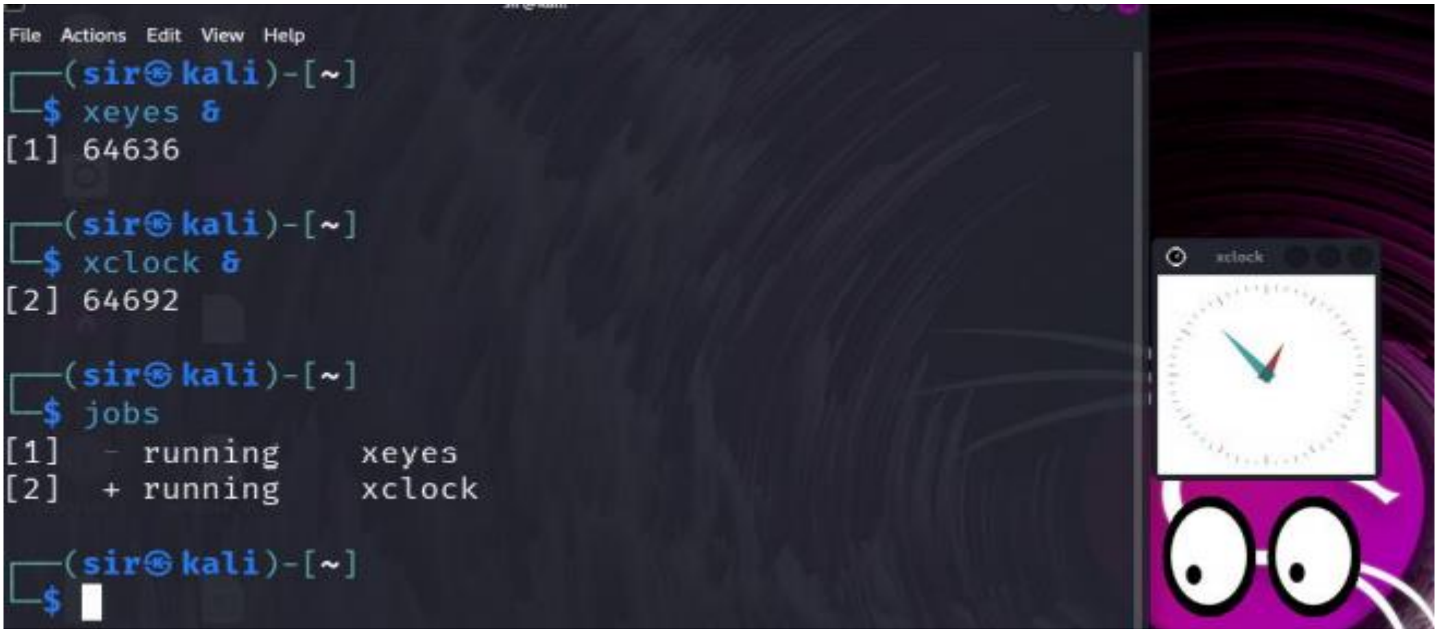
التحقق من مدة تشغيل النظام .



```
┌──(sir㉿kali)-[~]
└─$ uptime
 12:50:24 up  2:07,  1 user,  load average: 0.03, 0.12, 0.15

┌──(sir㉿kali)-[~]
└─$ █
```

42. List all jobs running in the background.

عرض جميع الوظائف الجارية في الخلفية:

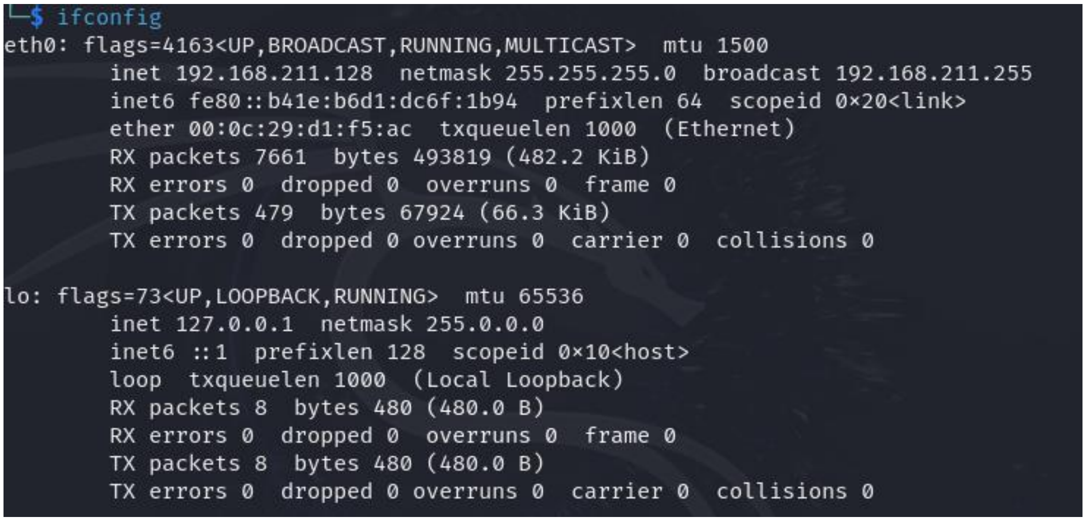


```
┌──(sir㉿kali)-[~]
└─$ xeyes &
[1] 64636

┌──(sir㉿kali)-[~]
└─$ xclock &
[2] 64692

┌──(sir㉿kali)-[~]
└─$ jobs
[1]  - running    xeyes
[2]  + running    xclock

┌──(sir㉿kali)-[~]
└─$ █
```

Section 5: Networking Commands

43. Display the network configuration.

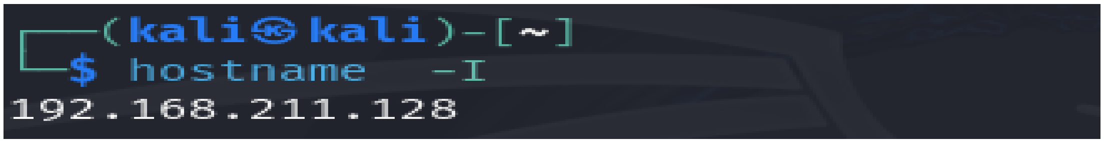
عرض إعدادات الشبكة:



```
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.211.128  netmask 255.255.255.0  broadcast 192.168.211.255
        inet6 fe80::b41e:b6d1:dc6f:1b94  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:d1:f5:ac  txqueuelen 1000  (Ethernet)
        RX packets 7661  bytes 493819 (482.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 479  bytes 67924 (66.3 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 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

44. Check the IP address of your machine

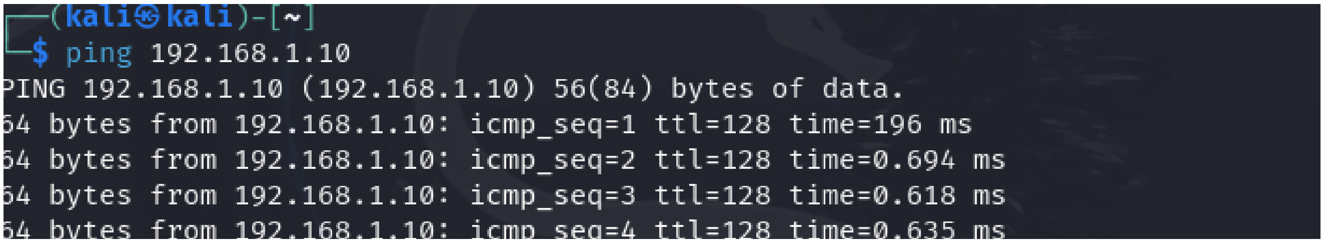
التحقق من عنوان IP للجهاز .



```
┌──(kali㉿kali)-[~]
└─$ hostname  -I
192.168.211.128
```

45. Test connectivity to an external server.

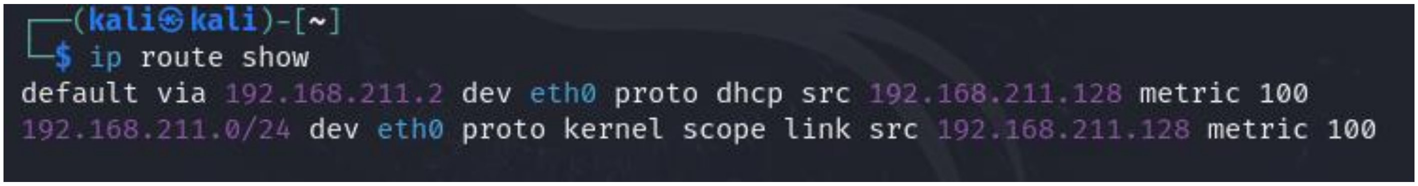
اختبار االتصال بسيرفر خارجي



```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.10
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=128 time=196 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=128 time=0.694 ms
64 bytes from 192.168.1.10: icmp_seq=3 ttl=128 time=0.618 ms
64 bytes from 192.168.1.10: icmp_seq=4 ttl=128 time=0.635 ms
```

46. Display the routing table.

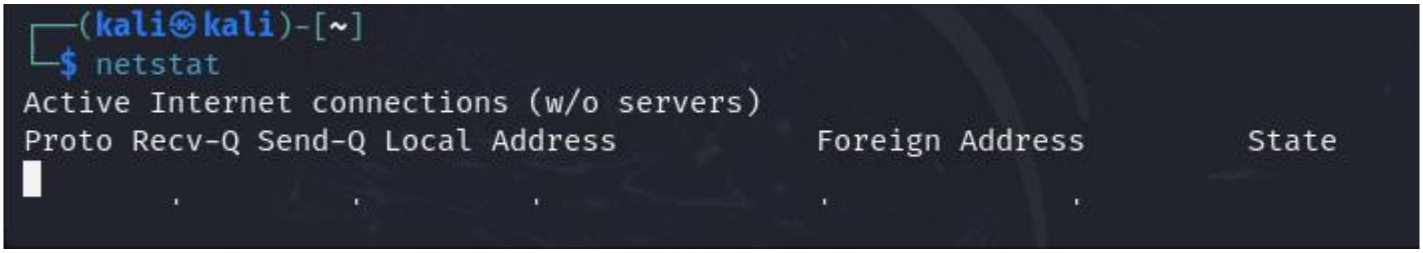
عرض جدول التوجيه



```
┌──(kali㉿kali)-[~]
└─$ ip route show
default via 192.168.211.2 dev eth0 proto dhcp src 192.168.211.128 metric 100
192.168.211.0/24 dev eth0 proto kernel scope link src 192.168.211.128 metric 100
```

47. Check the open ports and active connections

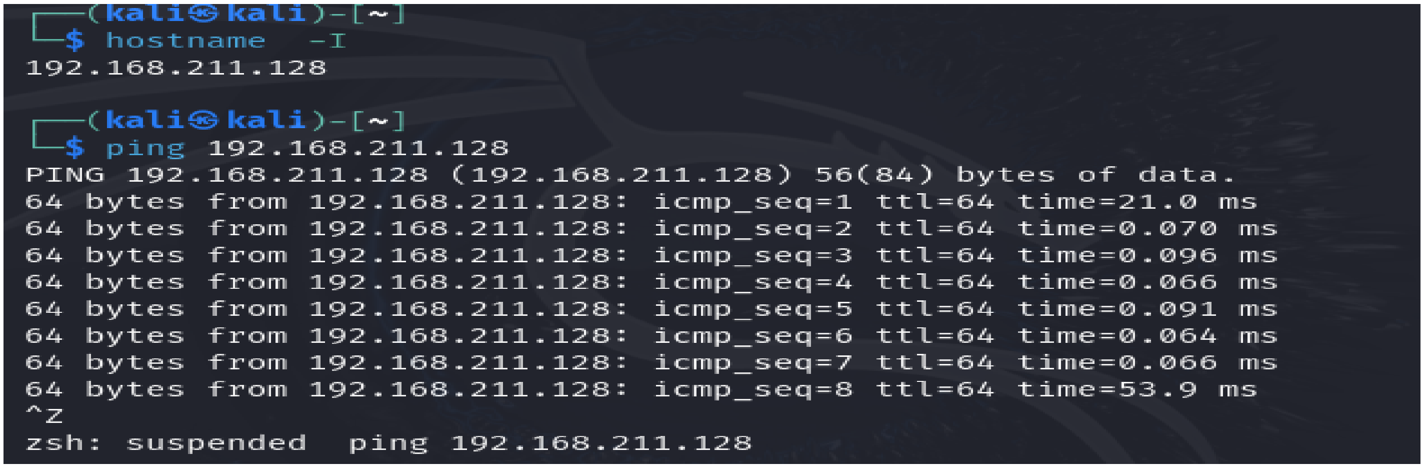
. التحقق من المنافذ المفتوحة واالتصاالت النشطة:



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

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

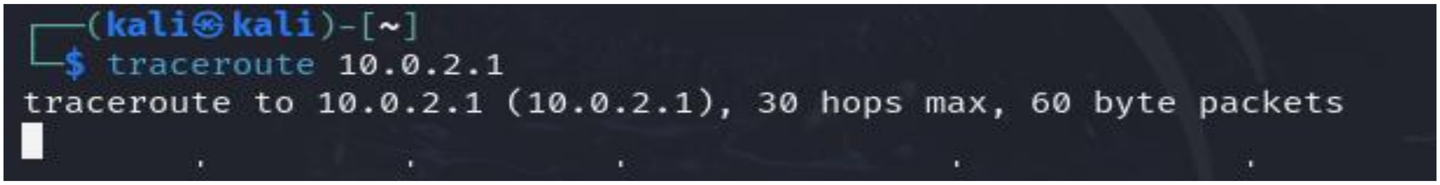
. عرض عنوان IP للجهاز والمضيف، والتحقق مما إذا كانا في نفس الشبكة:



```
┌──(kali㉿kali)-[~]
└─$ hostname  -I
192.168.211.128

┌──(kali㉿kali)-[~]
└─$ ping 192.168.211.128
PING 192.168.211.128 (192.168.211.128) 56(84) bytes of data.
64 bytes from 192.168.211.128: icmp_seq=1 ttl=64 time=21.0 ms
64 bytes from 192.168.211.128: icmp_seq=2 ttl=64 time=0.070 ms
64 bytes from 192.168.211.128: icmp_seq=3 ttl=64 time=0.096 ms
64 bytes from 192.168.211.128: icmp_seq=4 ttl=64 time=0.066 ms
64 bytes from 192.168.211.128: icmp_seq=5 ttl=64 time=0.091 ms
64 bytes from 192.168.211.128: icmp_seq=6 ttl=64 time=0.064 ms
64 bytes from 192.168.211.128: icmp_seq=7 ttl=64 time=0.066 ms
64 bytes from 192.168.211.128: icmp_seq=8 ttl=64 time=53.9 ms
^Z
zsh: suspended  ping 192.168.211.128
```

49. Trace the route to an external server.

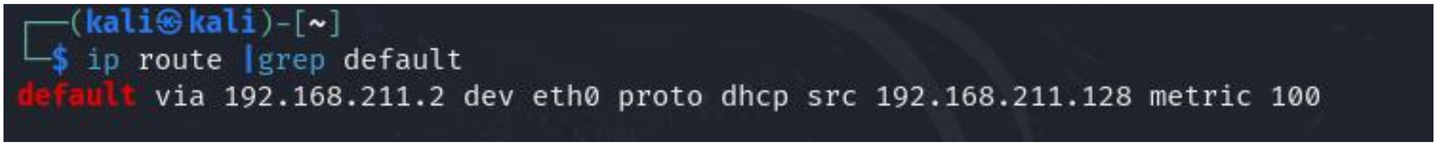
تتبع المسار إلى سيرفر خارجي :



```
┌──(kali㉿kali)-[~]
└─$ traceroute 10.0.2.1
traceroute to 10.0.2.1 (10.0.2.1), 30 hops max, 60 byte packets
```

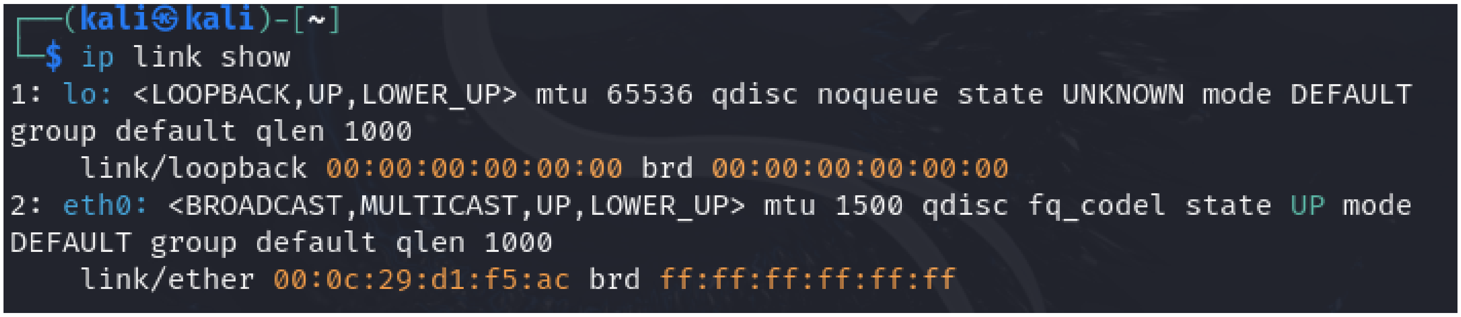
50. Find out the default gateway

. التحقق من بوابة العبور االفتراضية:



```
┌──(kali㉿kali)-[~]
└─$ ip route |grep default
default via 192.168.211.2 dev eth0 proto dhcp src 192.168.211.128 metric 100
```

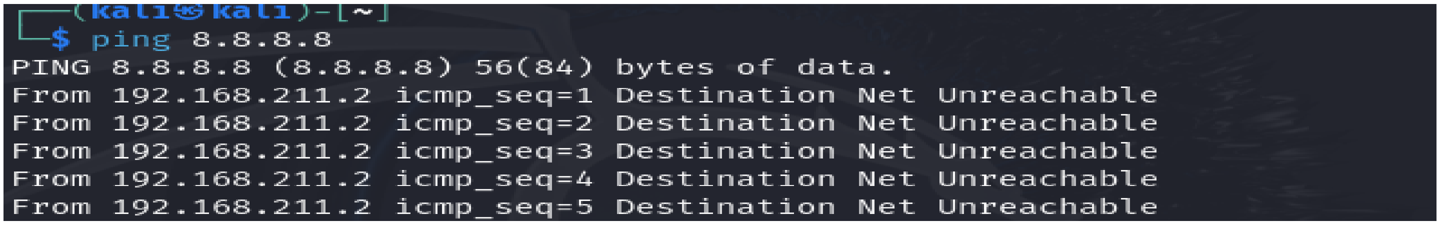
51-Check the MAC address of your network interface



```
┌──(kali㉿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 00:0c:29:d1:f5:ac brd ff:ff:ff:ff:ff:ff
```

52. Ensure that the VM can access external networks

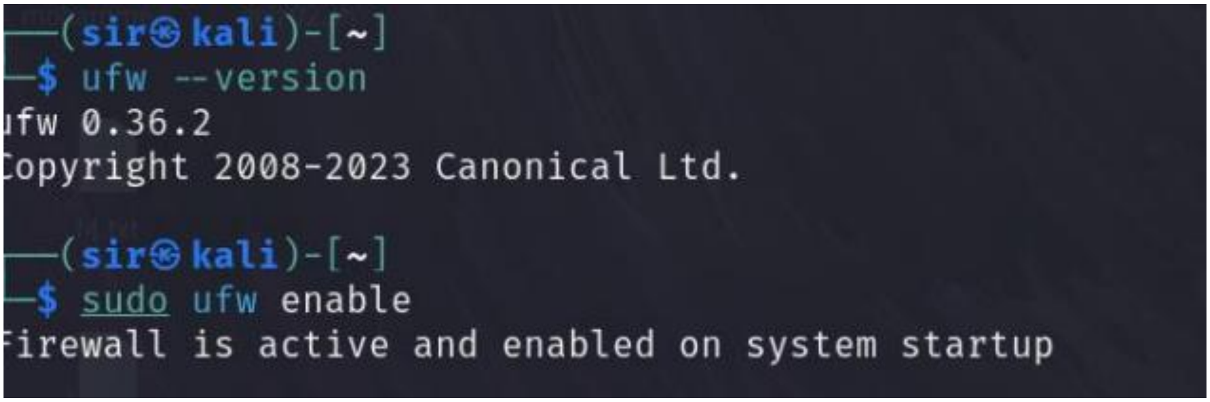
. التأكد من أن الجهاز االفتراضي يمكنه الوصول إلى الشبكات الخارجية:



```
┌──(kali㉿kali)-[~]
└─$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
From 192.168.211.2 icmp_seq=1 Destination Net Unreachable
From 192.168.211.2 icmp_seq=2 Destination Net Unreachable
From 192.168.211.2 icmp_seq=3 Destination Net Unreachable
From 192.168.211.2 icmp_seq=4 Destination Net Unreachable
From 192.168.211.2 icmp_seq=5 Destination Net Unreachable
```

Section 6: UFW Firewall

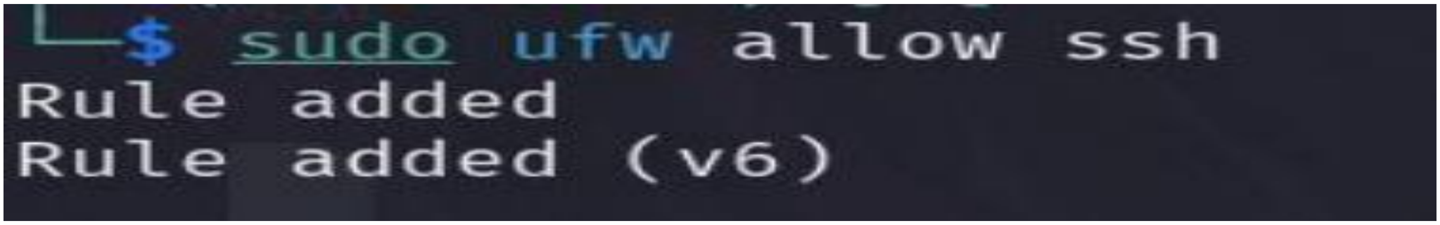
53. Enable the firewall.



```
──(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
```

54. Allow SSH connections through the firewall

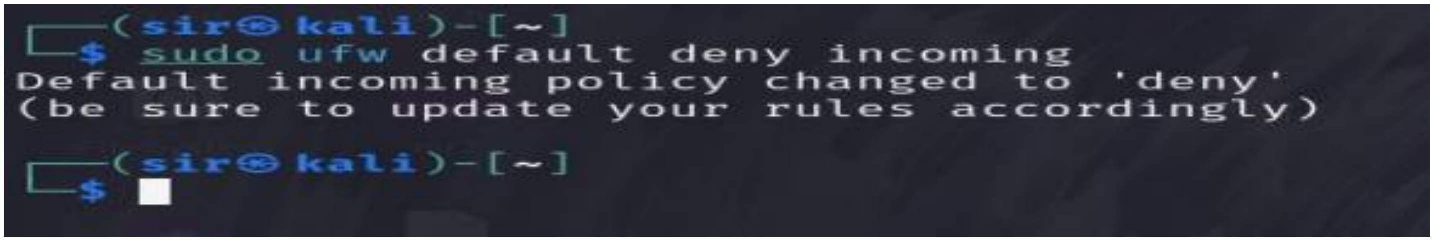
:من خالل الجدار الناري SSH السماح باتصاالت .



```
└─$ sudo ufw allow ssh
Rule added
Rule added (v6)
```

55. Deny all incoming traffic by default

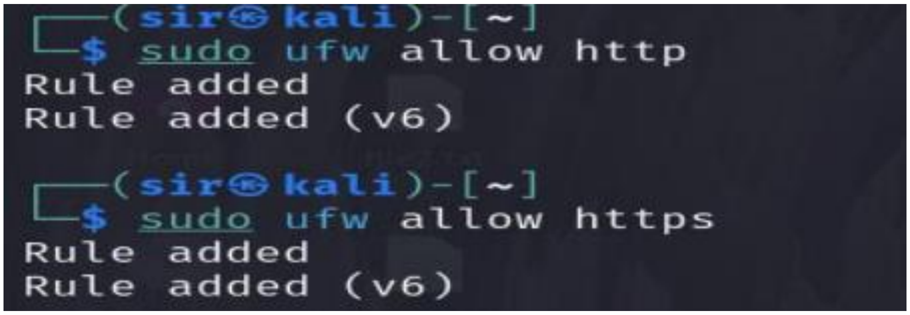
حظر جميع الحركات الواردة بشكل افتراضي .



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

┌──(sir㉿kali)-[~]
└─$ █
```

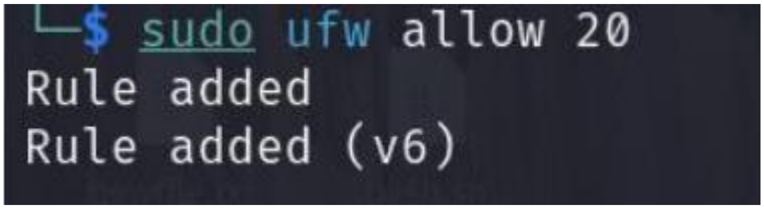
56. Allow HTTP and HTTPS traffic

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)
```

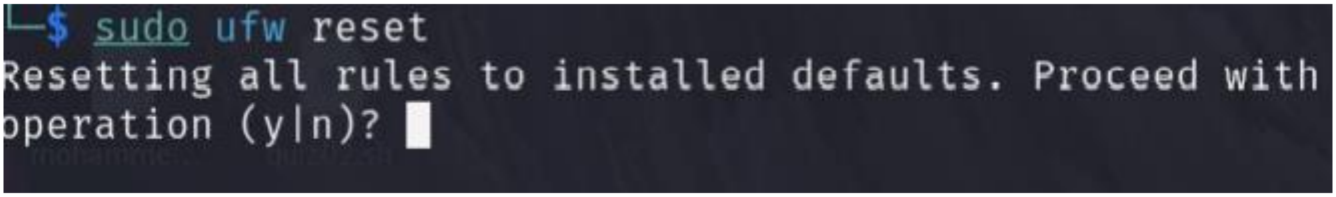
57. Allow port 20. السماح بالتصاالت عبر المنفذ 20



```
└─$ sudo ufw allow 20
Rule added
Rule added (v6)
```

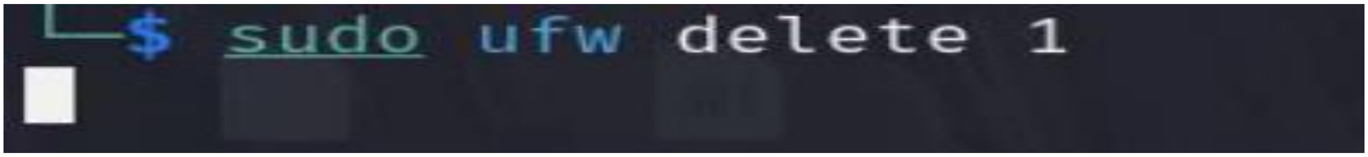
58. Reset the firewall settings.

إعادة تعيين إعدادات الجدار الناري



```
└─$ sudo ufw reset
Resetting all rules to installed defaults. Proceed with
operation (y|n)? █
```

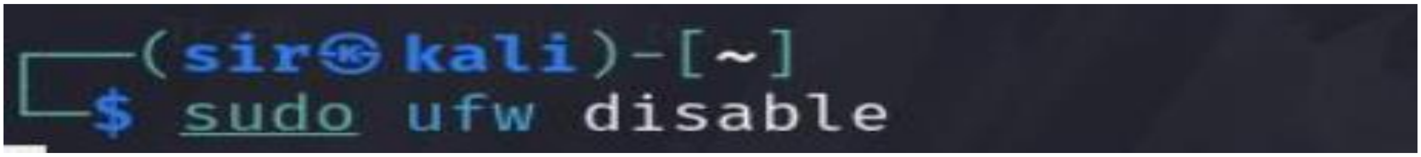
59. Delete a rule from the firewall. حذف قاعدة من قواعد الجدار الناري



```
└─$ sudo ufw delete 1
█
```

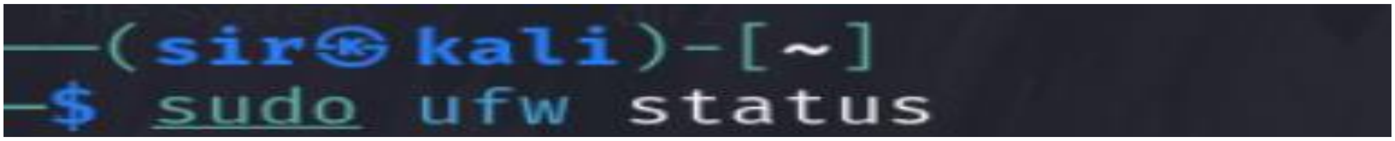
60. Disable the firewall

. تعطيل الجدار الناري:



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

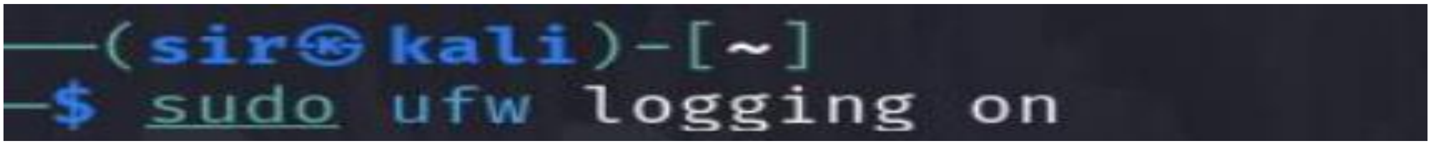
61. View the status of the firewall. عرض حالة الجدار الناري:



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

62. Log firewall activity and view it

. تسجيل نشاطات الجدار الناري وعرضها

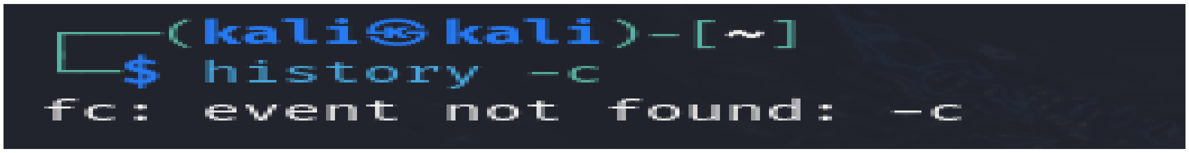


```
──(sir㉿kali)-[~]
─$ sudo ufw logging on
```

Section 7: Searching and System Information

63. Delete the command history.

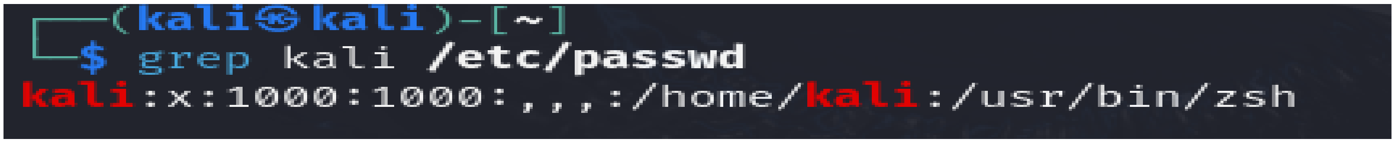
حذف تاريخ ألأوامر:



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

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

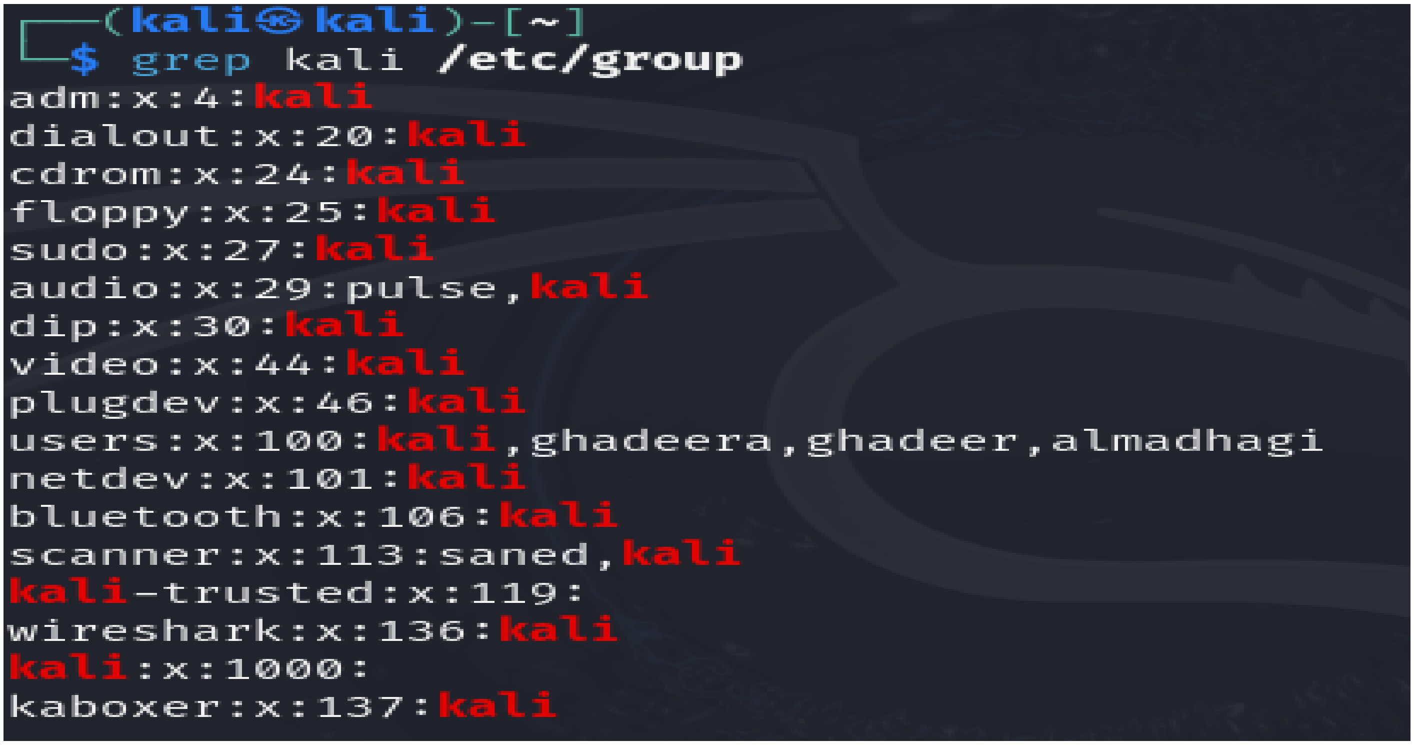
البحث عن كلمة "kali" في ملف `/passwd/etc



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

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

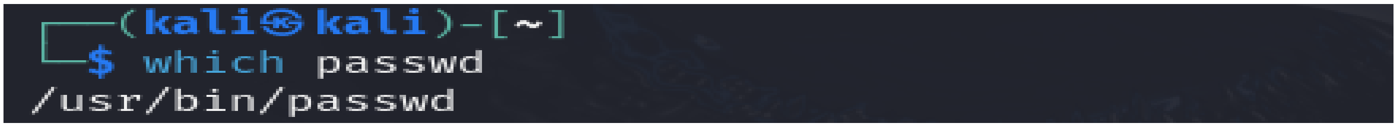
البحث عن كلمة "kali" في ملف `/group/et .



```
┌──(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
users:x:100:kali,ghadeera,ghadeer,almadhagi
netdev:x:101:kali
bluetooth:x:106:kali
scanner:x:113:saned,kali
kali-trusted:x:119:
wireshark:x:136:kali
kali:x:1000:
kaboxer:x:137:kali
```

66. Locate the `passwd` file.

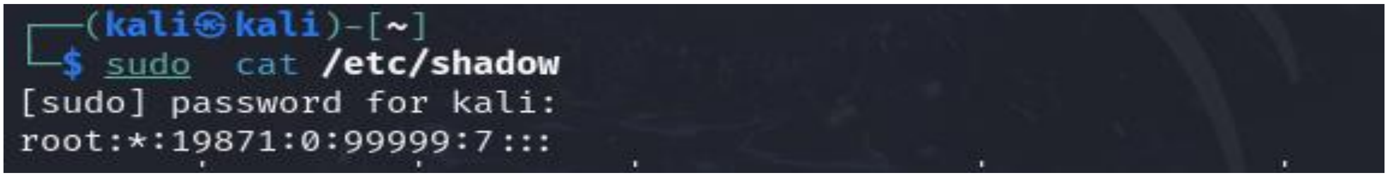
تحديد موقع ملف `passwd



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

67. Locate the shadow file and open it

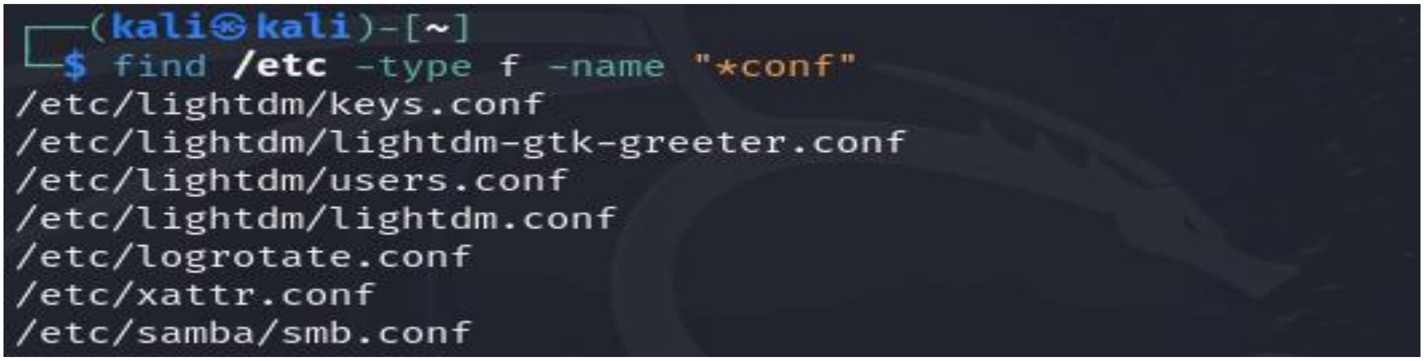
. تحديد موقع ملف `shadow `وفتحه:



```
┌──(kali㉿kali)-[~]
└─$ sudo  cat /etc/shadow
[sudo] password for kali:
root:*:19871:0:99999:7:::
```

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

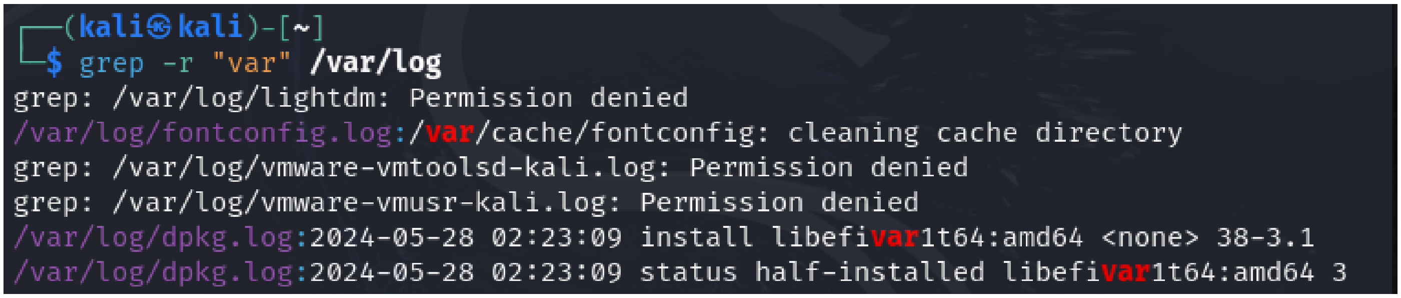
. البحث عن جميع ملفات التكوين في مجلد `/etc



```
┌──(kali㉿kali)-[~]
└─$ find /etc -type f -name "*conf"
/etc/lightdm/keys.conf
/etc/lightdm/lightdm-gtk-greeter.conf
/etc/lightdm/users.conf
/etc/lightdm/lightdm.conf
/etc/logrotate.conf
/etc/xattr.conf
/etc/samba/smb.conf
```

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

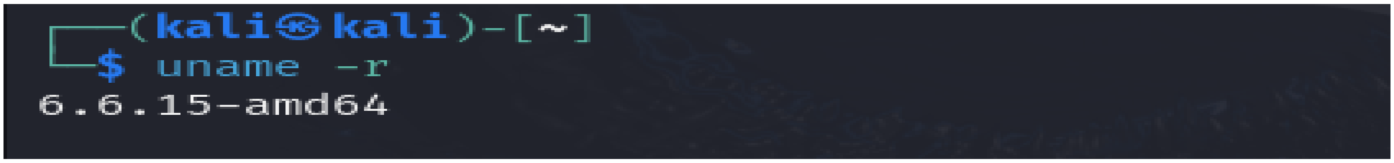
. البحث بشكل تكراري عن كلمة معينة في مجلد `/log/var



```
┌──(kali㉿kali)-[~]
└─$ grep -r "var" /var/log
grep: /var/log/lightdm: Permission denied
/var/log/fontconfig.log:/var/cache/fontconfig: cleaning cache directory
grep: /var/log/vmware-vmtoolsd-kali.log: Permission denied
grep: /var/log/vmware-vmusr-kali.log: Permission denied
/var/log/dpkg.log:2024-05-28 02:23:09 install libefivar1t64:amd64 <none> 38-3.1
/var/log/dpkg.log:2024-05-28 02:23:09 status half-installed libefivar1t64:amd64 3
```

70. View the system’s kernel version.

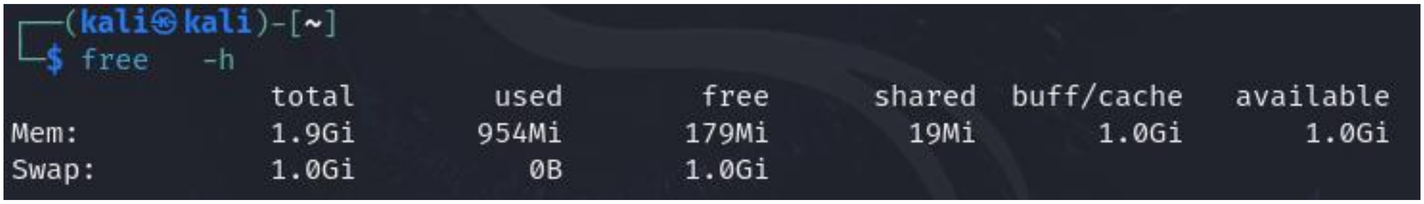
عرض إصدار نواة النظام



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

71. Display the system’s memory usage.

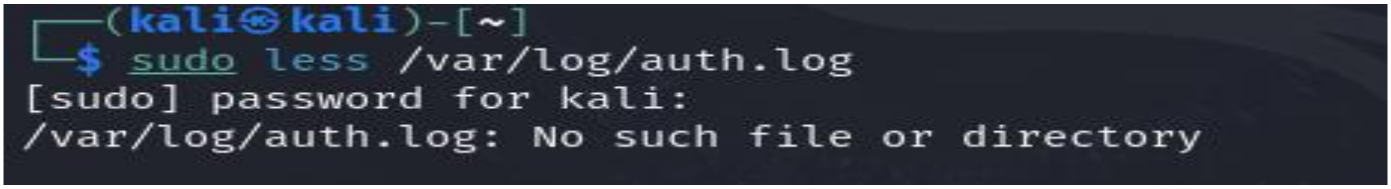
عرض استخدام الذاكرة في النظام



```
┌─(kali㉿kali)-[~]
└$ free  -h
               total        used        free      shared  buff/cache   available
Mem:           1.9Gi       954Mi       179Mi        19Mi       1.0Gi       1.0Gi
Swap:          1.0Gi          0B       1.0Gi
```

72. Show the system’s disk usage

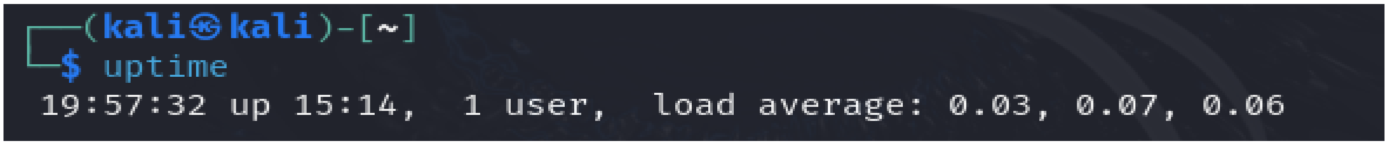
عرض استخدام القرص في النظام .



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

73. Check the system's uptime and load average

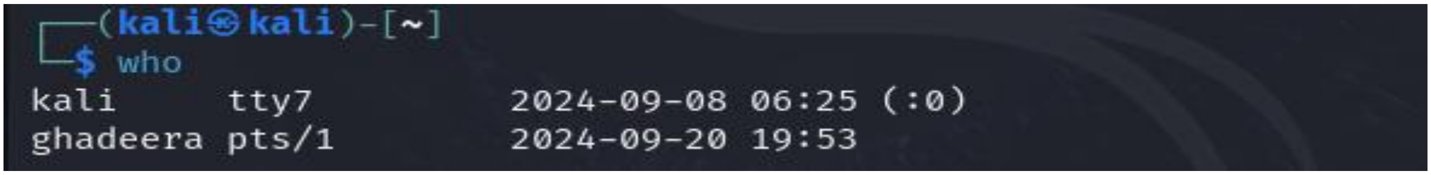
لتحقق من وقت تشغيل النظام ومتوسط الحمل: .



```
┌─(kali㉿kali)-[~]
└$ uptime
 19:57:32 up 15:14,  1 user,  load average: 0.03, 0.07, 0.06
```

74. Display the current logged-in users

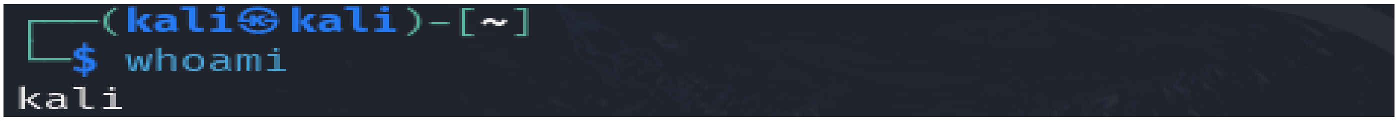
عرض المستخدمين الحاليين المسجلين في النظام .



```
┌──(kali㉿kali)-[~]
└─$ who
kali     tty7         2024-09-08 06:25 (:0)
ghadeera pts/1        2024-09-20 19:53
```

75. Check the identity of the current user.

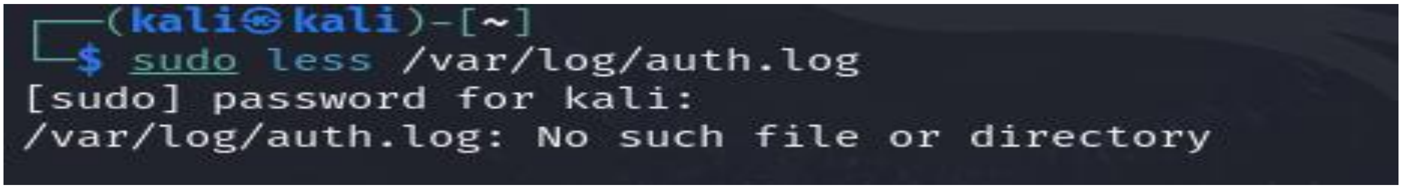
التحقق من هوية المستخدم الحالي



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

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

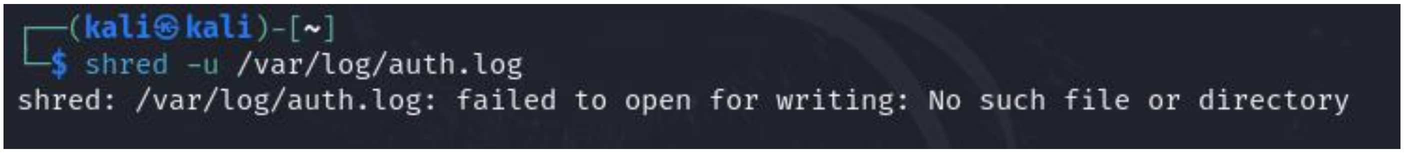
عرض ملف `/ var/log/auth.log`: .



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

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

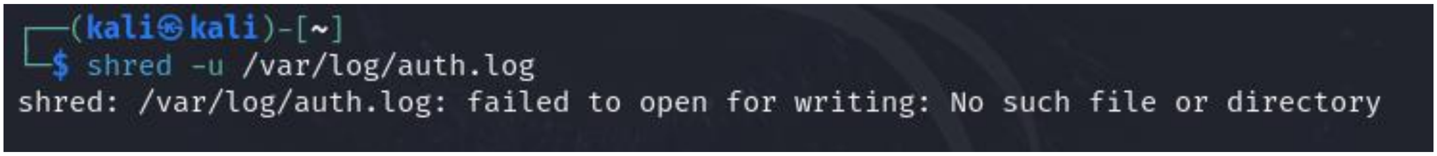
تقطيع ملف `log.auth` بشكل آمن:



```
┌──(kali㉿kali)-[~]
└─$ 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

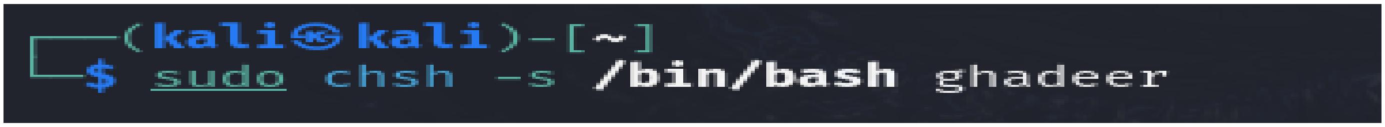
. كيفية قفل حساب مستخدم لمنعه من تسجيل الدخول:



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

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

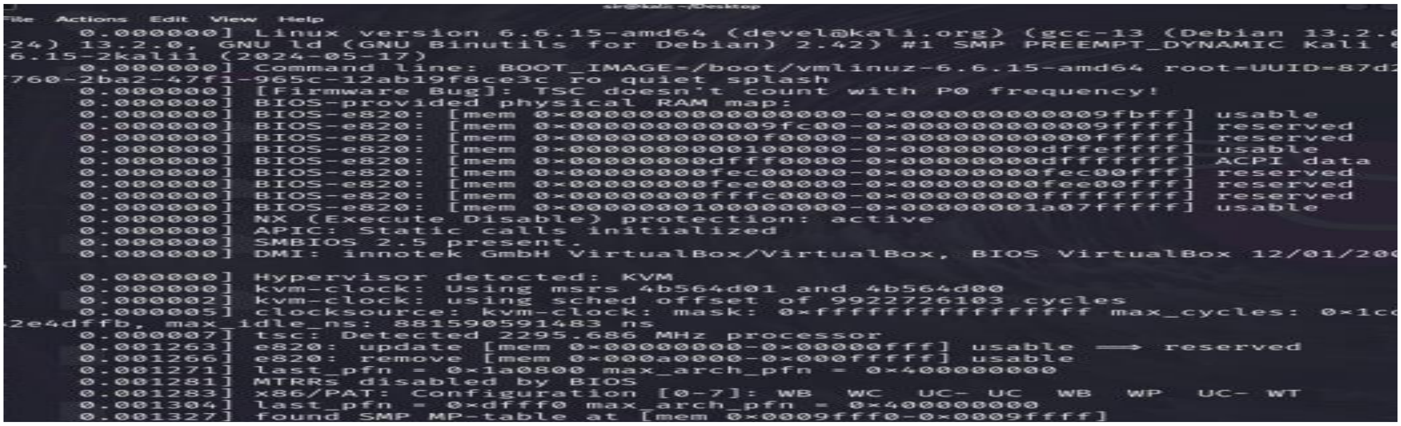
. تغيير الصدفة االفتراضية لمستخدم:



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

80. Display the system's boot messages

. عرض رسائل اإلقالع للنظام



```
     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
.
     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
2e4dffb, 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]
```

تم بحمد الله

Prepared By Eng	*Ghadeer Almadahi*
Subject	*Cyber Security*
teacher	*Eng. Abdulrazzaq Al-Samawi*