



KALI LINUX

The Weapon of Security Against Cyber Challenges

اللهم علّمنا ما ينفعنا، وانفعنا بما علّمتنا، وزدنا علماً.

أنا طالب في مجال الأمن السيبراني، أطمح إلى تطوير نفسي والسير بثبات في هذا التخصص الحيوي والمليء بالتحديات

ومن منطلق حيي لنشر الفائدة، أشارك ما أتعلّمه من أدوات، تطبيقات، ومصادر مفيدة – لعلها تكون عوناً لكل من يسعى للتعلّم أو يبدأ خطواته في هذا المجال

قد لا أملك الكثير من الخبرات، ولكن أملك الرغبة الصادقة في مشاركة ما أعرفه، ومساعدة كل من يرغب في التعلّم.

ويكفيني شرفاً أن أتمثل بقول النبي ﷺ:

"أفضل الصدقة أن يتعلم المرء علماً ثم يعلّمه أخاه المسلم"

وإذا كنت بحاجة لشرح أو توضيح لأي أداة أو موضوع في مجال الأمن السيبراني، لا تتردد في التواصل معي، وسأكون سعيداً بمساعدتك بكل ما أستطيع.

للتواصل عبر البريد: 

techhamd@gmail.com

قناتي على تليجرام – روابط، أدوات، تطبيقات، وكل ما يفيد المتعلمين: 

t.me/TechHamd

الفهرس

1. [المقدمة](#)
2. [مميزات Kali Linux](#)
3. [استخدامات Kali Linux](#)
4. [طريقة تنصيب Kali Linux](#)
5. [تعريف الواجهة الرسومية لـ Kali Linux](#)
6. [الأوامر الأساسية في Kali Linux](#)
7. [التسلسل الهرمي لنظام Kali Linux](#)
8. [أوضاع الوصول](#)
9. [أوامر الإيقاف والتشغيل لـ Kali Linux](#)
10. [إدارة حسابات المستخدمين والمجموعات](#)
11. [ماهو sudo ؟](#)
12. [خطوات هامة عند تثبيت Kali Linux](#)
13. [أهم أدوات Kali Linux](#)
14. [أنواع الملفات](#)
15. [تعديل الأذونات](#)
16. [أوامر Kali Linux](#)
17. [إختصارات Kali Linux \(في لوحة المفاتيح\)](#)
18. [الخاتمة](#)

بسم الله الرحمن الرحيم

الحمد لله وبعد:

في عصر التكنولوجيا الحديثة، حيث أصبحت الشبكات والأنظمة الرقمية جزءاً أساسياً من حياتنا اليومية، أصبحت مسائل الأمان السيبراني أكثر أهمية من أي وقت مضى. يتعين على الأفراد والمؤسسات والشركات أن يكونوا على استعداد دائم لحماية بياناتهم وأصولهم الرقمية من التهديدات السيبرانية المتزايدة.

تزايدت التهديدات السيبرانية في التعقيد والتطور، وأصبح من الضروري الاستعداد للتصدي لهذه التحديات بفعالية، هذا هو المكان الذي يأتي فيه نظام **Kali Linux** إلى الواجهة.

س / ما هو نظام **Kali Linux** ومتى تأسس؟ وماهي مميزاته واستخداماته؟

Kali Linux من أشهر التوزيعات لنظام **Linux**، وهو مشروع مفتوح المصدر ومجاني وينتمي إلى عائلة

Debian Linux، تم اعلان صدوره من قبل شركة **Offensive Security** عام 2013، صمم خصيصاً لأختبار

الأمان، و اختراق الانظمة، واكتشاف الثغرات والضعف في الأنظمة، إنه النظام الأساسية المستخدمة بشكل شائع في مجال الأمان السيبراني.

مميزات Kali Linux:

يحتوي على مجموعة كبير من الأدوات:

يأتي مزوداً بأكثر من 600 أداة متخصصة في مجال الأمان السيبراني، تشمل هذه الأدوات: أدوات اختراق الشبكات وتحليل الثغرات وفحص الأمان والتجسس والعديد من التقنيات الأخرى.

دورات تدريبية ومستندات:

يقدم دعماً شاملاً للمستخدمين من خلال مجتمع نشط [بموقع الويب الخاص به](#)، توجد دورات تدريبية ومواد تعليمية متاحة للمستخدمين في تعلم كيفية تثبيت واستخدام الأدوات.

توافق الأجهزة:

يمكن تثبيتها على مجموعة متنوعة من الأجهزة بما في ذلك الكمبيوترات المكتبية وأجهزة الكمبيوتر المحمول وأجهزة **Raspberry PI**.

مفتوح المصدر:

متاح كتوزيع مفتوح المصدر وهذا يعني أنه يمكن للمطورين تخصيصه وتعديله وتوجيهه بحرية لتلبية احتياجاتهم الخاصة.

استخدامات Kali Linux:

اختبار الاختراق:

هو الأداة الرئيسية المستخدمة لاختبار الأمان والكشف عن الثغرات في الأنظمة والشبكات، يمكن استخدامه لاختبار الثغرات واختبار الاختراق على أنظمة مختلفة.

الاختبار الأمني:

يستخدم لتقييم الأمان السيبراني لأنظمة المعلومات والشبكات، وذلك من خلال فحص النقاط الضعيفة واكتشاف الثغرات.

اختبار الشبكات:

يستخدم لاختبار أمان الشبكات واكتشاف الأخطاء في تكوين الشبكات وأجهزة التوجيه.

اختبار الاختراق الاجتماعي:

يمكن استخدام **Kali Linux** لإجراء هجمات اجتماعية محاكاة بهدف اختبار مقدرة المؤسسة على مقاومة هذا النوع من الهجمات.

البحث عن ثغرات:

فحص الأنظمة والتطبيقات بحثاً عن ثغرات معروفة.

تعليم الأمن السيبراني:

يستخدم **Kali Linux** في العديد من البرامج التعليمية والدورات التدريبية لتدريس أساسيات ومهارات الأمن السيبراني.

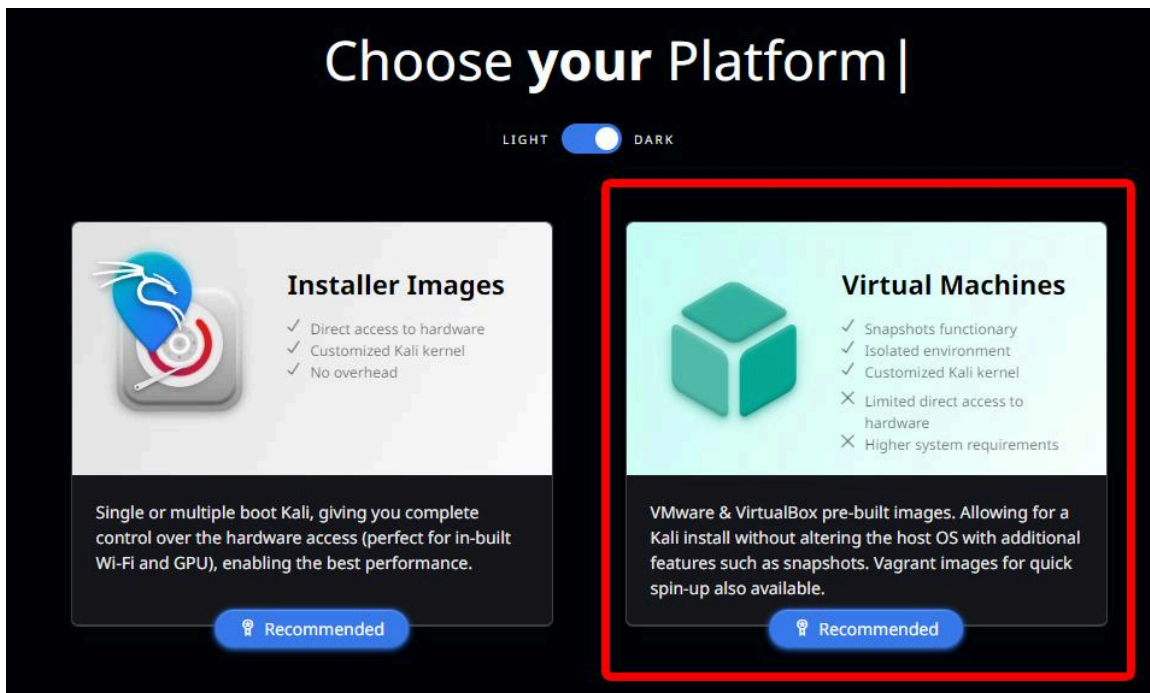
طريقة تنصيب Kali Linux على VMware Workstation

1- الدخول الى الموقع الخاص بـ [kali Linux](https://www.kali.org/) <https://www.kali.org/>

ثم الضغط على **DOWNLOAD**



ثم اختيار **Virtual Machines**

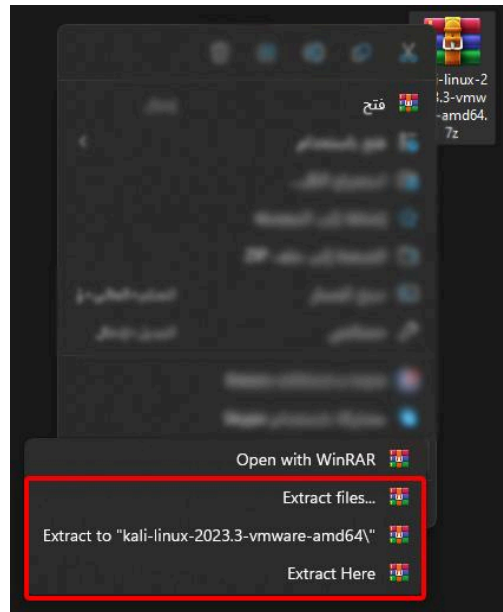
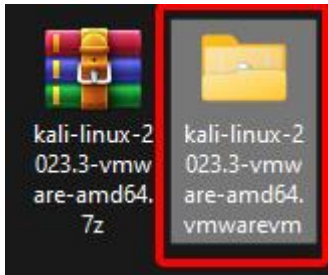


اختار نوع وحدة الجهاز الخاص بك **32 - 64 bit** ثم قم باختيار **VMware**

يمكنك أيضاً اختيار برامج افتراضية مماثلة لـ **VMware** كالـ **VirtualBox - Hyper - QEMU**



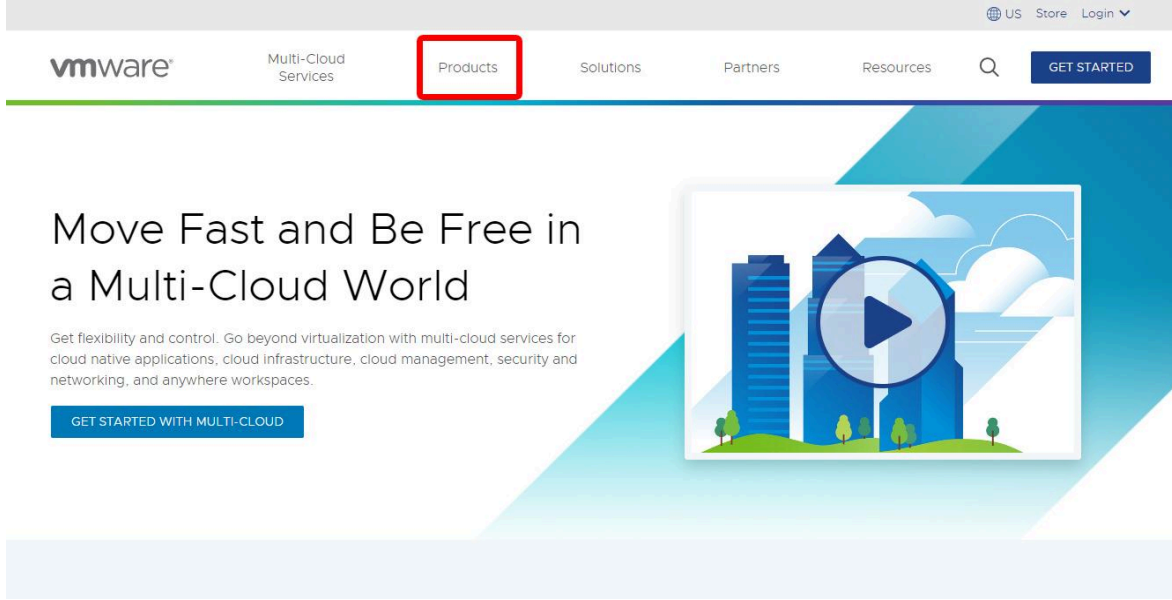
بعد انتهاء التحميل استخراج الملف



2- تحميل برنامج VMware Workstation

الدخول الى الموقع [/https://www.vmware.com](https://www.vmware.com)

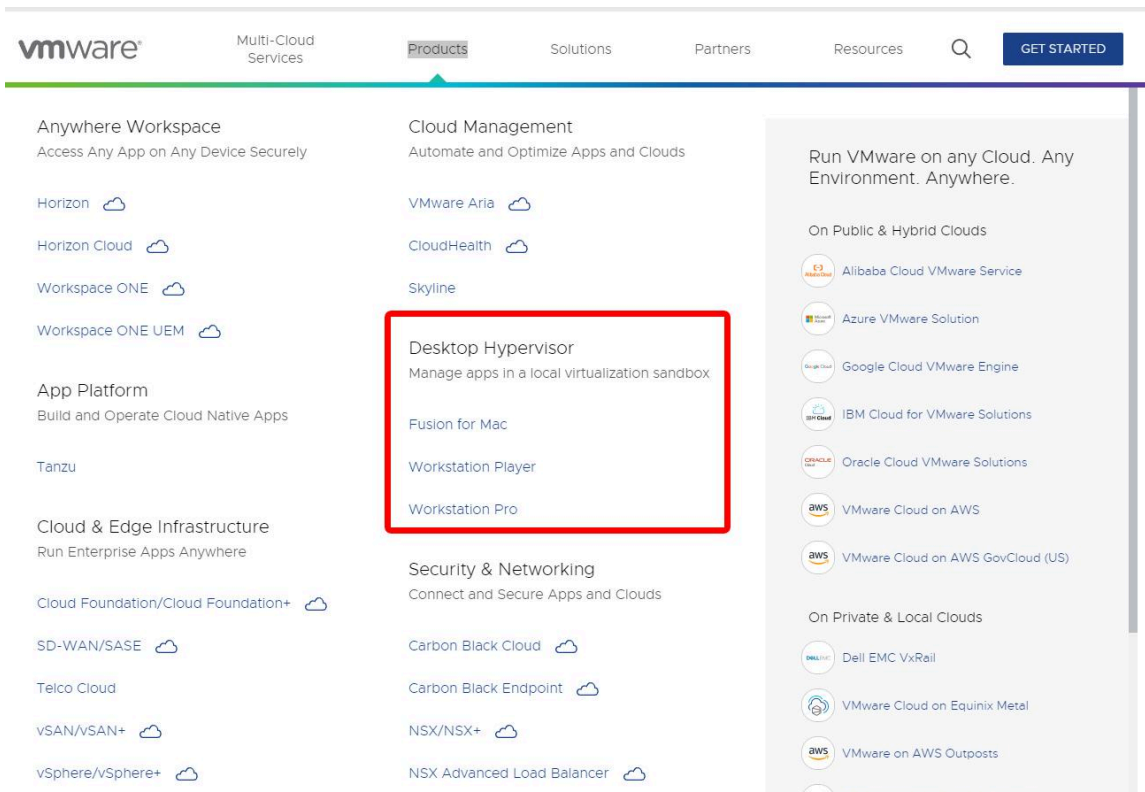
ثم الانتقال إلى **Products**



يتوفر **vmware** بنسختين:

Workstation Player مجانية باسم

ومدفوعة باسم **Workstation Pro**



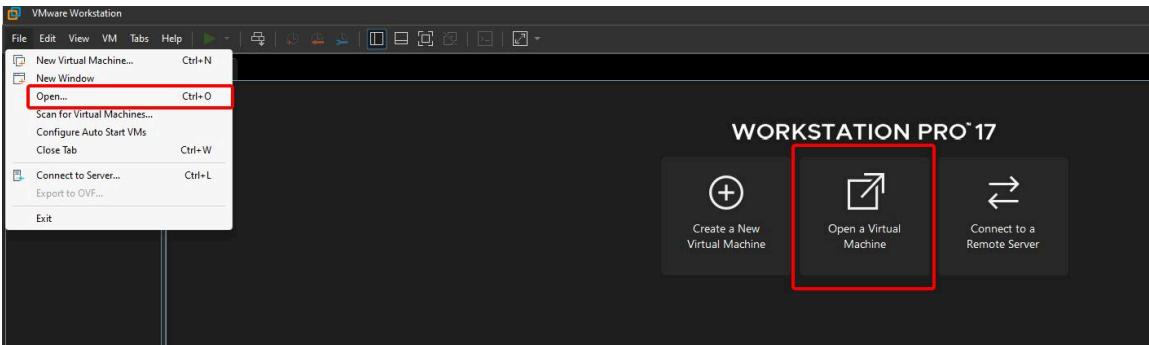


س/ ما الفرق بين النسخة المجانية والمدفوعة ؟

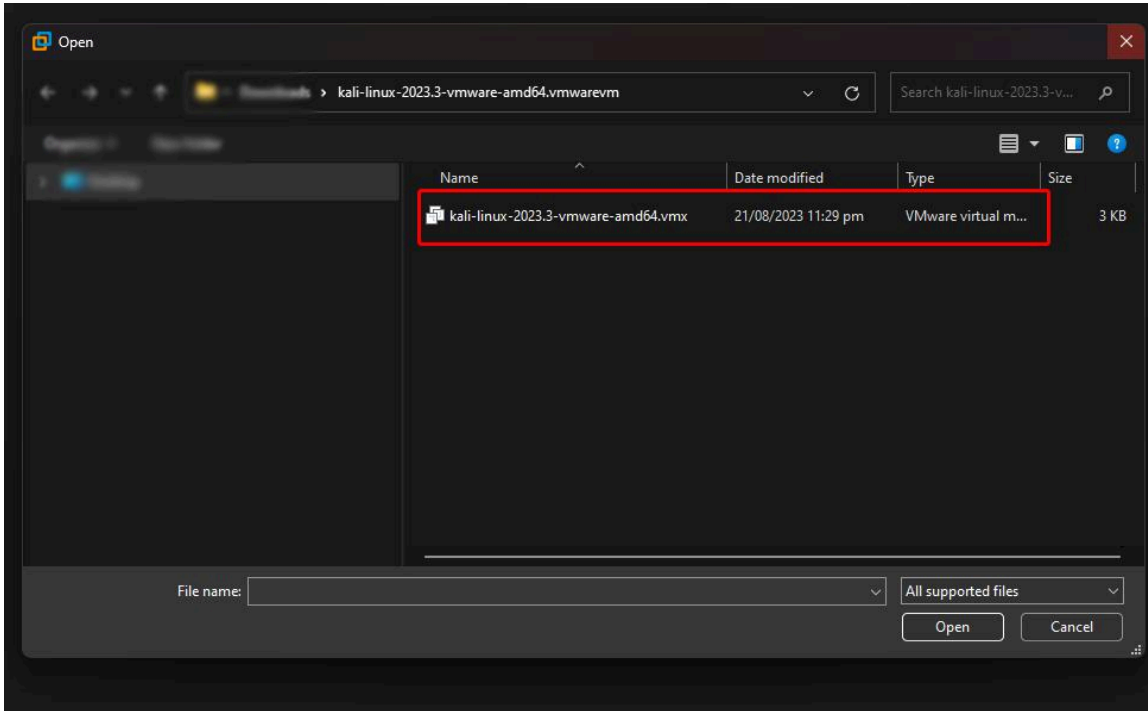
ج/ الفرق بالنسخة المدفوعة تأتي بميزة الـ **Snapshot Manager** وهي ميزة للأشياء نسخ احتياطية للأجهزة الافتراضية.

بعد تحميل وتنصيب البرنامج على الجهاز الخاص بك

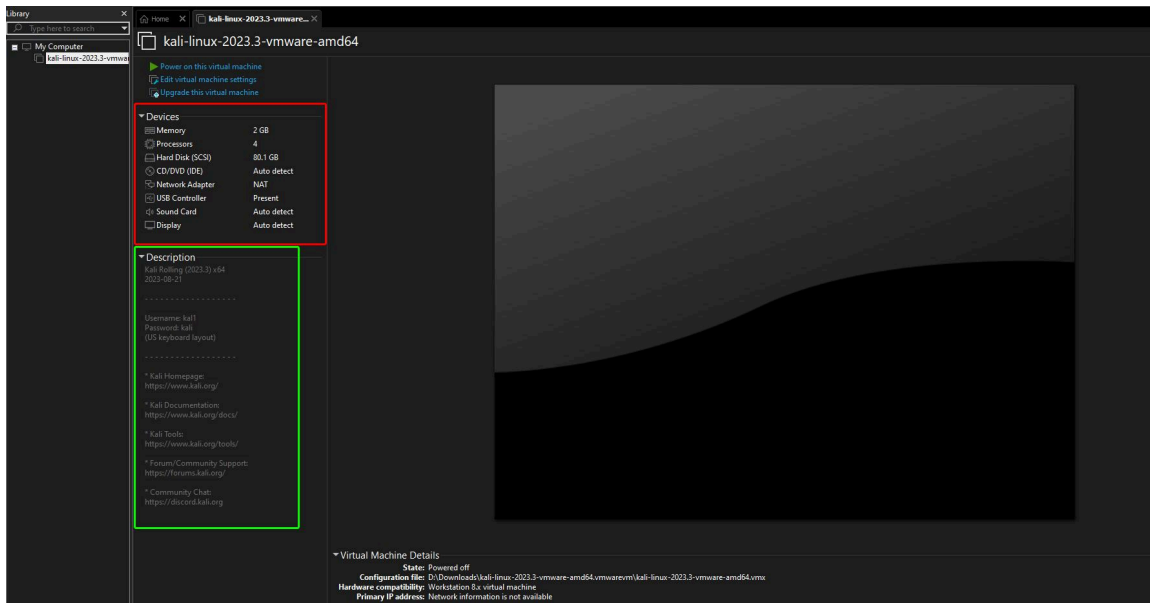
تنصيب **Kali Linux** اختيار **Open a Virtual Machine** أو الاختصار على لوحة التحكم **Ctrl + O**



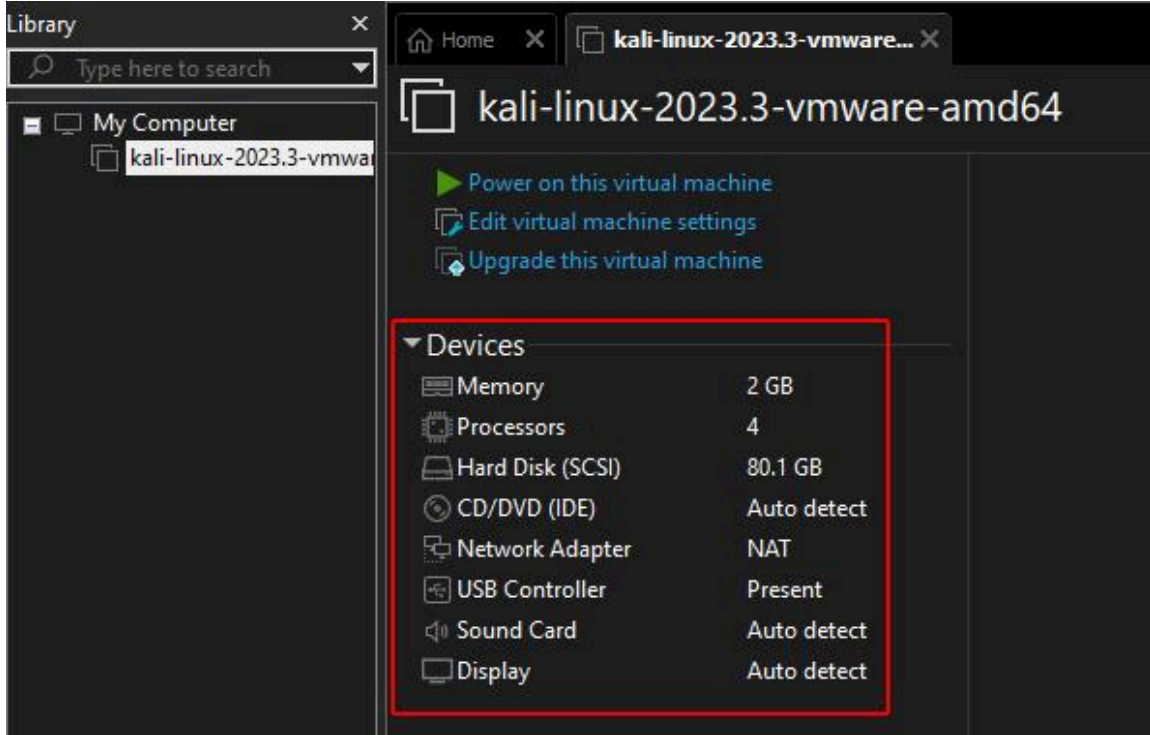
اختيار الملف المستخرج



بعد اختيار الملف ستظهر الصفحة التالية:



يحتوي قسم **Devices** على مواصفات نظام **Kali Linux** (يفضل عدم تغييرها)



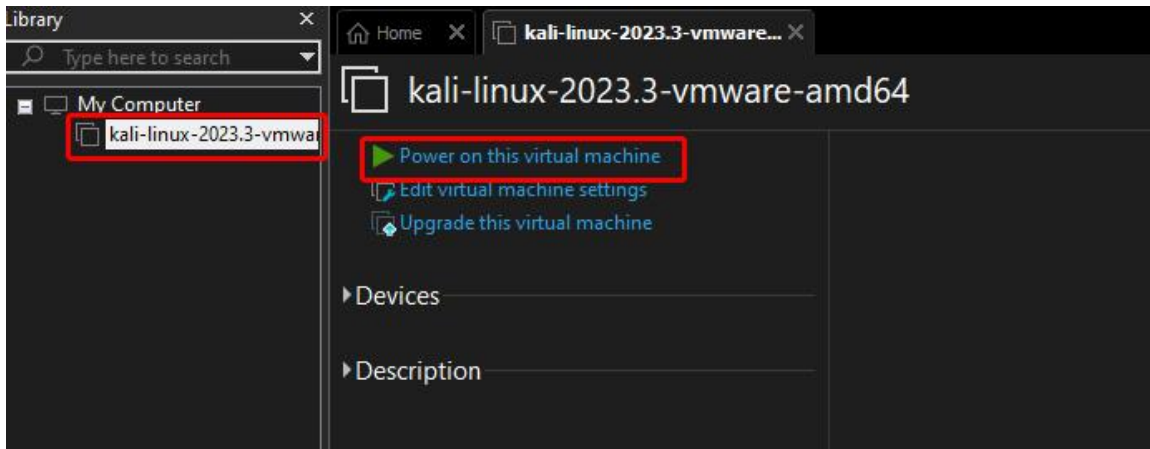
س/ ما هي المواصفات التي تشغل نظام Kali Linux ؟

ج/ نظام **Kali Linux** لا يحتاج الى مواصفات عالية لتشغيله، يمكن تشغيله على ذاكرة **1GB** ومعالج بتردد **1GHz** ومساحة تخزين لا تقل عن **20GB**.

يحتوي قسم **Description** على معلومات النظام كال **Username** و **Password** الخاصة بـ **Kali** و [موقع الرسمي للنظام](#)، و [مواقع الأدوات الخاصة](#)، و [موقع دردشة المجتمع](#).

لتشغيل **Kali Linux**:

اختيار **kali-linux** ثم **Power on this virtual**



بعد التشغيل يجب اختيار **Kali Linux** بالضغط على زر Enter او الانتظار 5 ثواني للدخول تلقائياً



عند التشغيل سيطلب منك Username و Password للدخول

س/ ما هو Username و Password لنظام Kali وهل تستطيع تغييرها ؟

ج/ نعم يمكن تغييرها

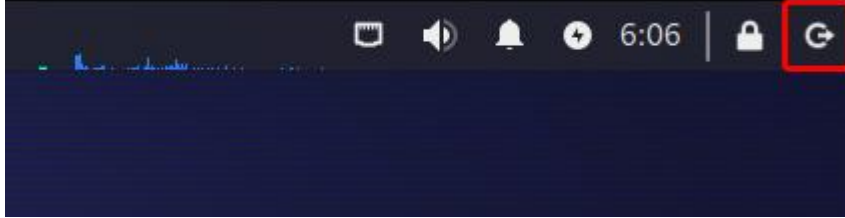


عند وصولك الى هذا المرحلة يمكنك البدء باستخدام Kali Linux 🐉

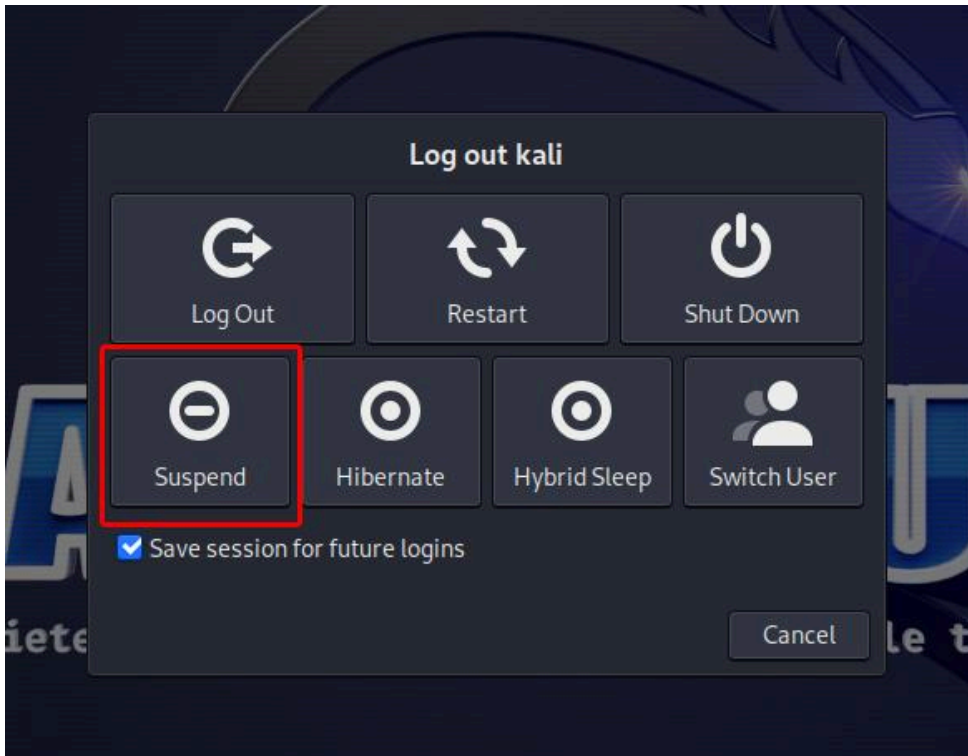


تعريف الواجهة الرسومية لـ Kali Linux

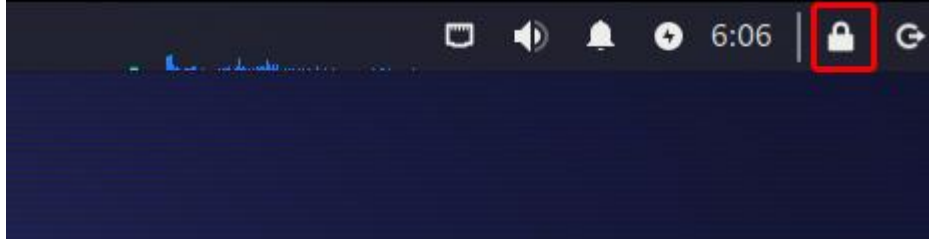
تدل الايقونة ادناه الى تسجيل الخروج من النظام



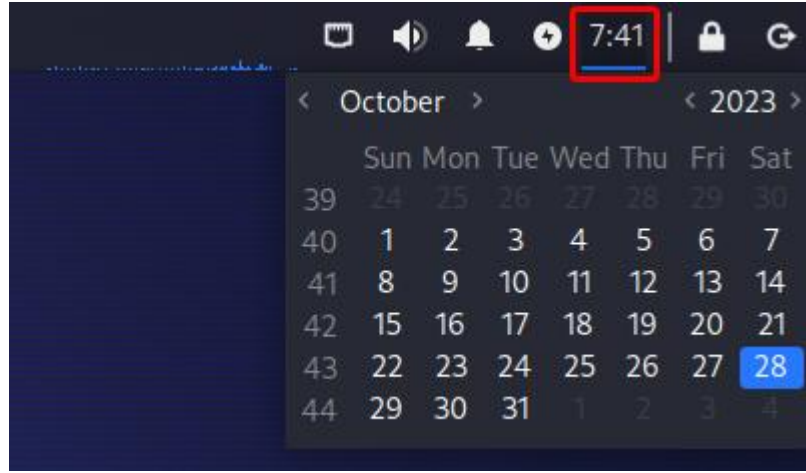
(يفضل عند تسجيل الخروج من النظام اختيار **Suspend**)



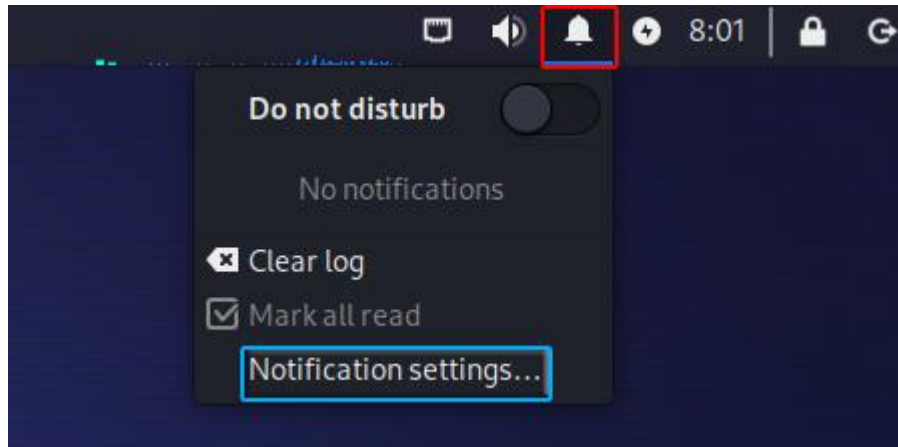
تدل الايقونة ادناه **Lock Screen** إلى إيقاف الشاشة



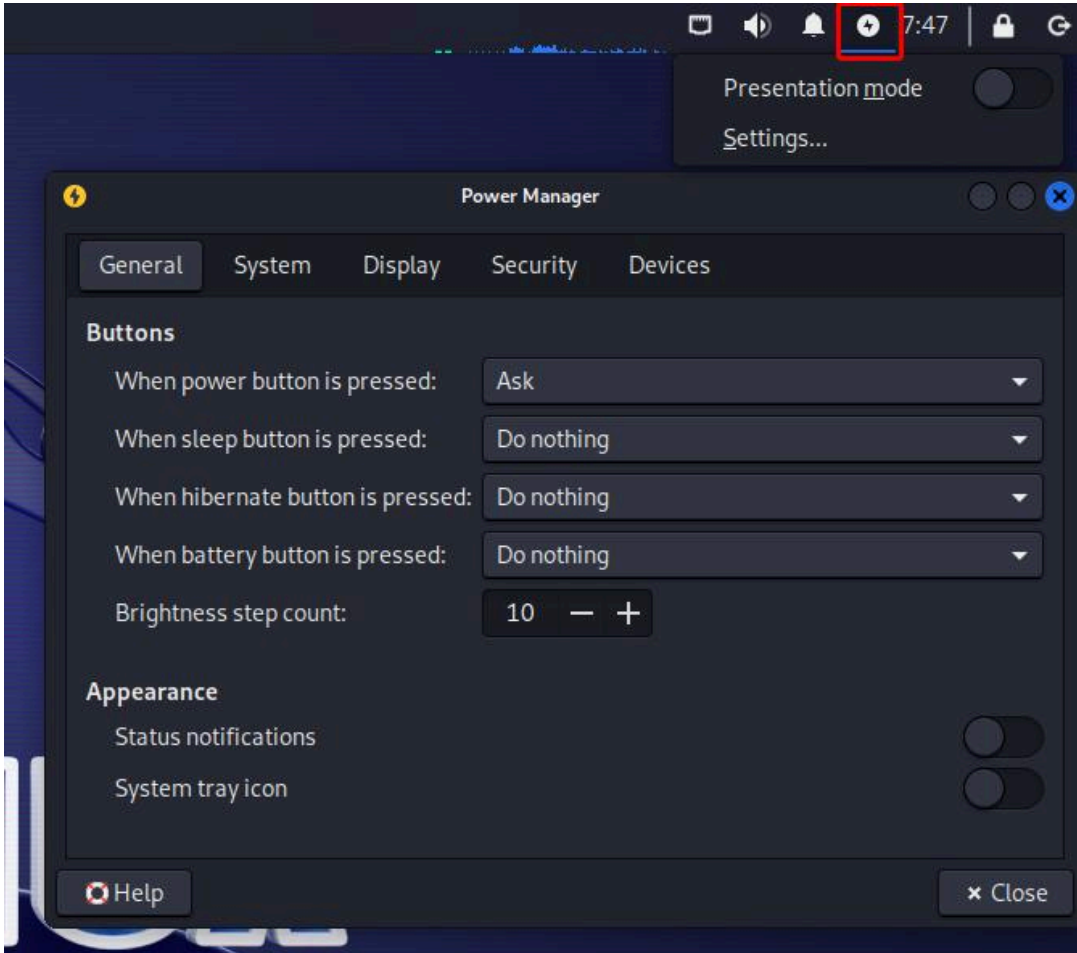
تدل الايقونة ادناه **The Date** إلى الوقت والتاريخ



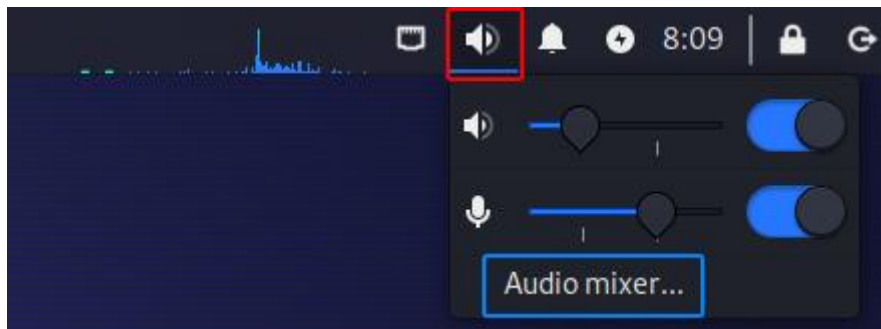
تدل الايقونة ادناه **Notifications** إلى الإشعارات في النظام، يمكن تغيير التحكم في الإشعارات من خلال **Notifications settings**



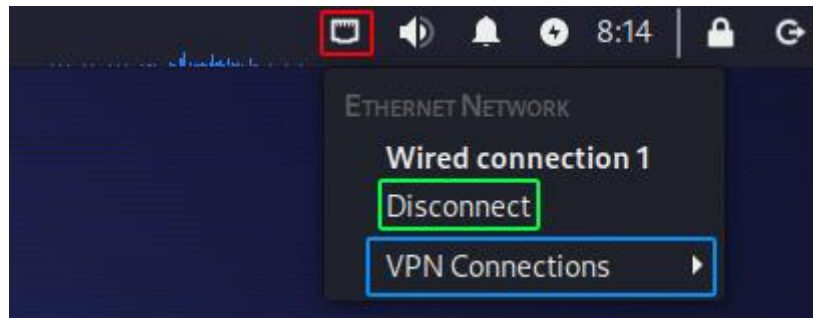
تدل الايقونة ادناه **Power Manager** إلى مدير الطاقة، والذي يمكنه أن يشمل العديد من الوظائف والإعدادات، ضبط إعدادات السطوع، إدارة وضع السكون، تخصيص إعدادات الطاقة.



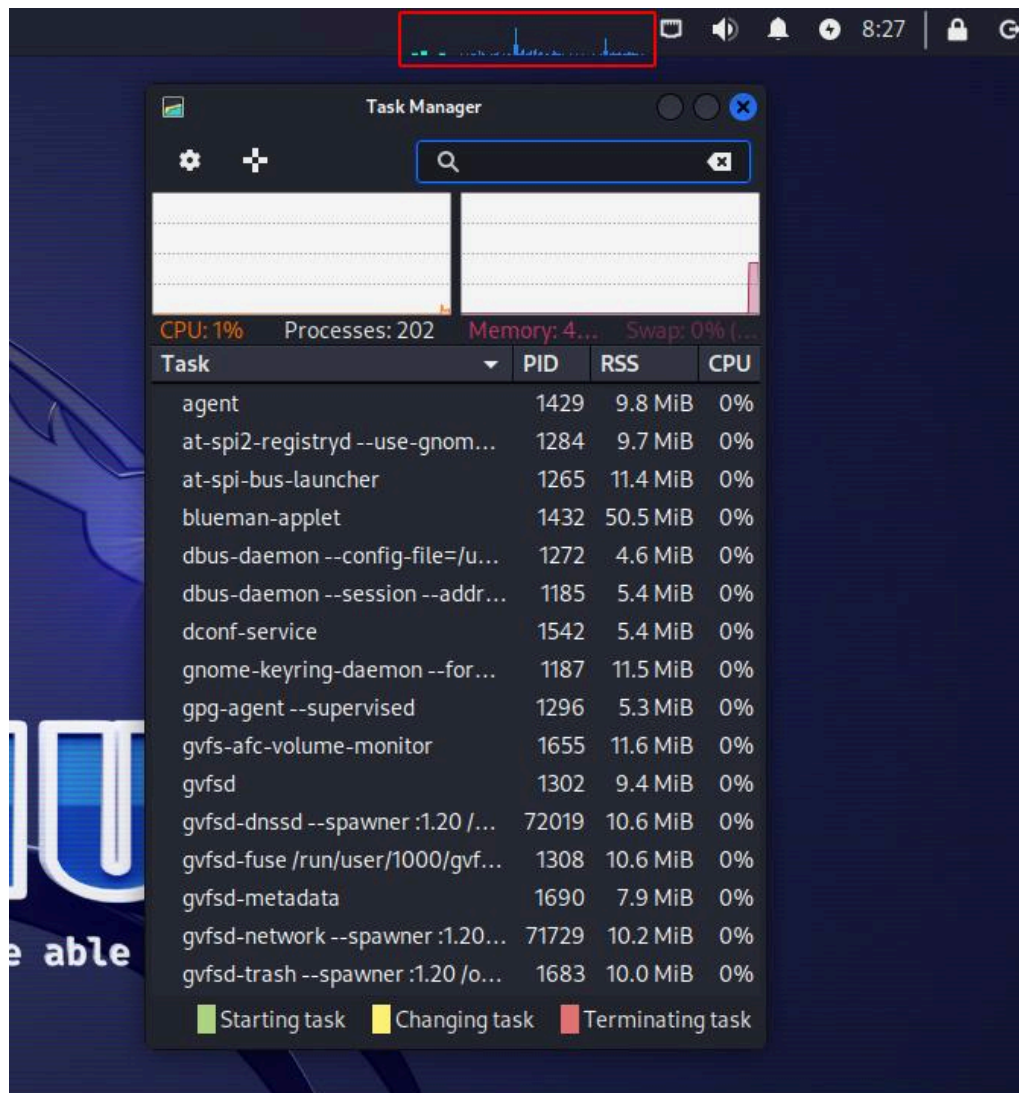
تدل الايقونة ادناه **The Sound** إلى نسبة الصوت والميكروفون في النظام، يمكن ضبط إعدادات الصوت من خلال **Audio mixer**



تدل الايقونة ادناه **ETHERNET NETWORK** إلى الانترنت المتصل بالنظام، حيث يمكن قطع الانترنت من خلال **Disconnect**، أو الإتصال بالـ **VPN** من خلال **VPN Connections**.



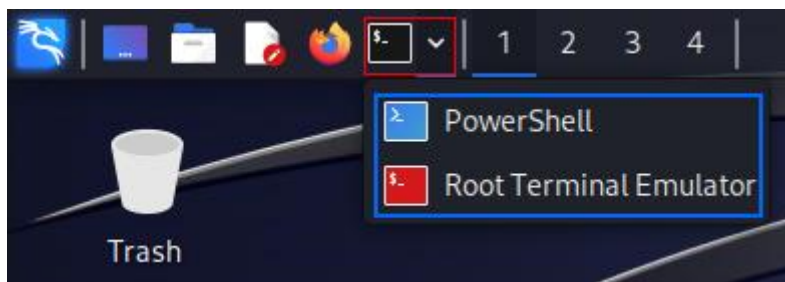
تدل الايقونة ادناه **Task Manager** إلى مراقبة وإدارة العمليات والمهام واستهلاك الموارد على النظام، تسمح بإنهاء العمليات، وهي مفيدة لأغراض الاختبار والتشخيص وإدارة المواد.



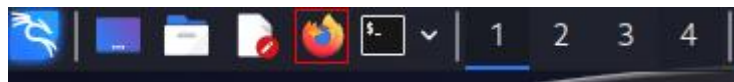
على الجهة اليسرى توجد أيقونات أخرى منها، أيقونة **New desktop** لإنشاء سطح مكتب آخر كما موضح ادناه.



تدل الايقونة ادناه الى **terminal emulator** أو المعروفة بالشاشة السوداء الخاصة بالأوامر، يمكن بالنقر على السهم الدخول الى الشاشة الزرقاء او **PowerShell**، أو الدخول إلى **Root terminal** أو الشاشة السوداء بصلاحيات **Root** (المالك)



تدل الايقونة ادناه الى برنامج التصفح **Firefox**، لتصفح شبكة الإنترنت العالمية.



س/ هل يمكن تثبيت متصفحات اخرى غير **Firefox** ؟

ج/ نعم يمكن تثبيت متصفحات اخرى كـ **Google Chrome** و **Brave** واخرى.

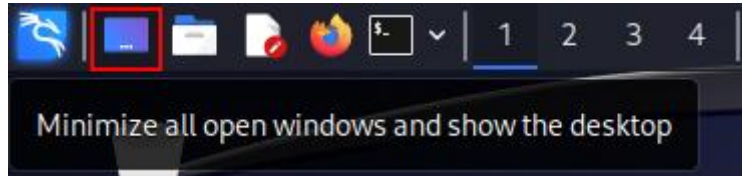
تدل الايقونة ادناه الى **Text Editor**، محرر نصوص للكتابة.



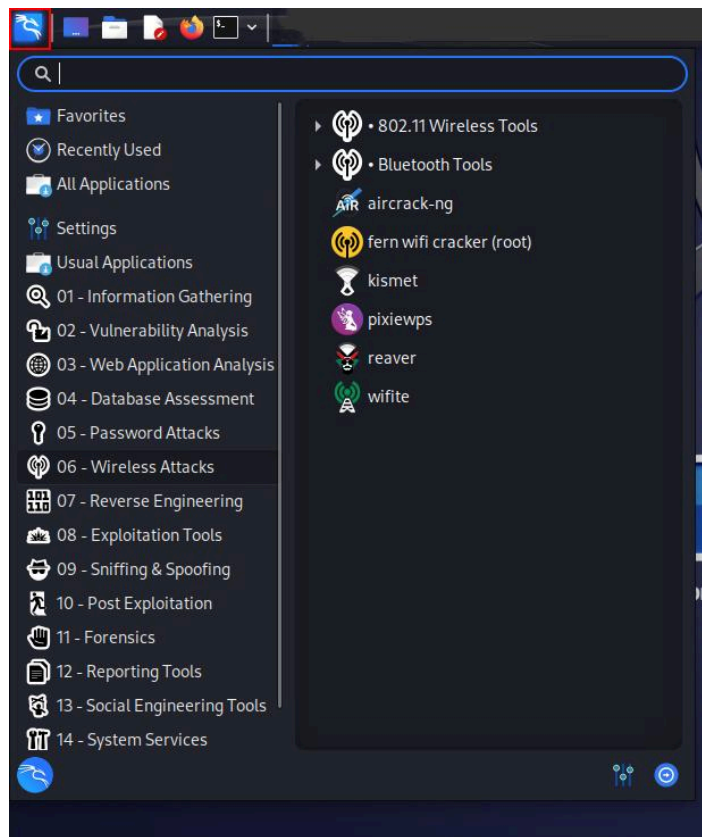
تدل الايقونة ادناه الى **home/kali/**، لاختصار التنقل بين المجلدات و إنشاء مجلدات جديدة



تدل الايقونة ادناه الى اخفاء جميع النوافذ المفتوحة وإظهار سطح المكتب.



تدل الايقونة ادناه الى جميع الأدوات والبرامج المثبتة والغير مثبتة في نظام **Kali**.

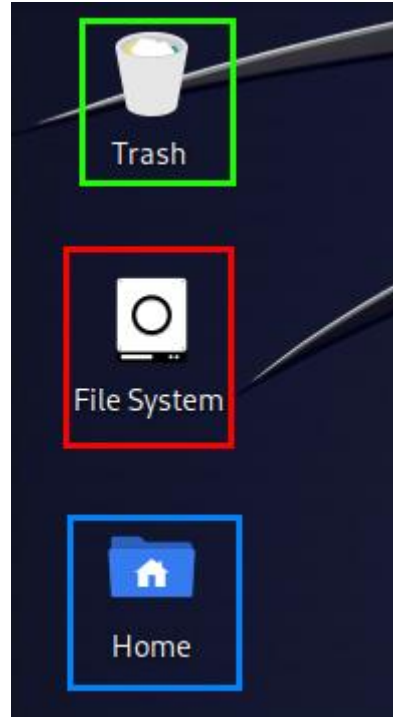


تدل الايقونات الاخرى الى:

سلة المحذوفات: تحتوي على الملفات التي تم حذفها من النظام.

ملفات النظام: يحتوي على جميع ملفات النظام.

سطح المكتب: يحتوي على ملفات سطح المكتب الأساسية.

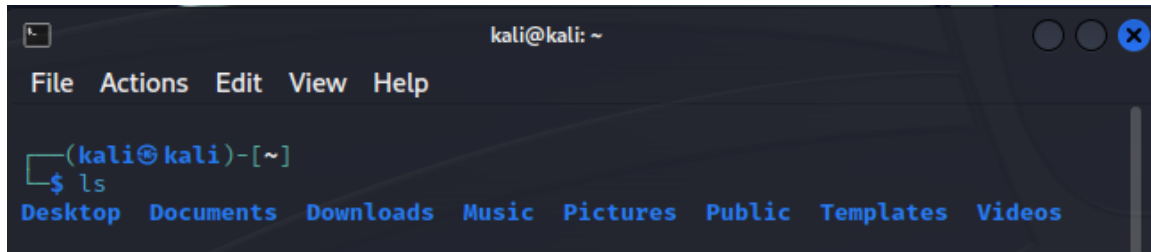


الأوامر الأساسية في نظام Kali Linux

يستخدم لعرض المجلد الحالي: **pwd** (Print Working Directory)

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
└─$ pwd  
/home/kali  
(kali@kali)-[~]  
└─$
```

يستخدم لعرض محتوى المجلد الحالي: **ls** (List)

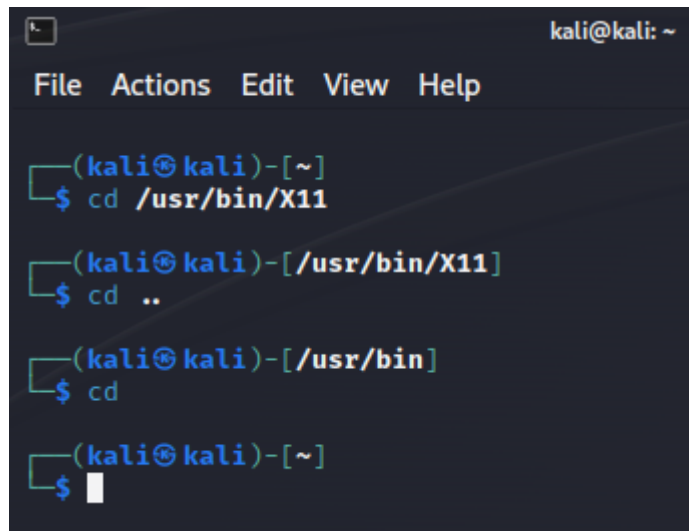


```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
└─$ ls  
Desktop Documents Downloads Music Pictures Public Templates Videos
```

يستخدم للانتقال بين المجلدات: **cd** (Change Directory)

الرجوع خطوة الى الوراء **cd ..**

الرجوع الى الملف الرئيسي **cd**



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
└─$ cd /usr/bin/X11  
(kali@kali)-[/usr/bin/X11]  
└─$ cd ..  
(kali@kali)-[/usr/bin]  
└─$ cd  
(kali@kali)-[~]  
└─$
```

يستخدم لإنشاء مجلد جديد: **mkdir** (Make Directory)



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
└─$ mkdir text  
(kali@kali)-[~]  
└─$ ls  
Desktop Downloads Pictures Templates Videos  
Documents Music Public text
```

rmdir (Remove Directory): يستخدم لحذف مجلد فارغ:

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
└─$ ls  
Desktop Downloads Pictures Templates Videos  
Documents Music Public text  
  
(kali@kali)-[~]  
└─$ rmdir text  
  
(kali@kali)-[~]  
└─$ ls  
Desktop Documents Downloads Music Pictures Public Templates Videos
```

rm (Remove): يستخدم لحذف ملف أو مجلد:

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
└─$ ls  
Desktop Downloads Pictures Templates Videos  
Documents Music Public text  
  
(kali@kali)-[~]  
└─$ rm test  
  
(kali@kali)-[~]  
└─$ ls  
Desktop Documents Downloads Music Pictures Public Templates Videos
```

س/ ماهو الفرق بين أمر rmdir و rm ؟

ج/ أمر **rmdir** مستخدم لحذف الدلائل المجلدات الفارغة، إذا حاولت استخدام "**rmdir**" لحذف مجلد يحتوي على ملفات أو مجلدات داخله، ستتلقى رسالة خطأ تشير إلى أن المجلد ليس فارغاً.

أمر **rm** مستخدم لحذف الملفات والمجلدات الفارغة وإيضاً لحذف المحتوى، بما في ذلك الملفات والمجلدات داخلها.

يستخدم لإنشاء ملف جديد: **touch**

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

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

(kali@kali)-[~]
└─$ touch test

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

يستخدم لنسخ ملف أو مجلد: **cp (Copy)**

كما موضح ادناه تم نقل الملف **test** الى المجلد **test1**

```
kali@kali: ~/text1
File Actions Edit View Help

(kali@kali)-[~]
└─$ ls
Desktop Downloads Pictures Templates text1
Documents Music Public test Videos

(kali@kali)-[~]
└─$ cp test text1

(kali@kali)-[~]
└─$ cd text1

(kali@kali)-[~/text1]
└─$ ls
test
```

يستخدم لعرض محتوى ملف نصي: **cat**

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

(kali@kali)-[~]
└─$ cat test
You are welcome, I love you very much
```

يستخدم لمسح الأوامر من الشاشة: **clear**:

يستخدم لتنفيذ أمر بصلاحيات المسؤول **root**: **sudo**:

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
└─$ apt install nmap  
E: Could not open lock file /var/lib/dpkg/lock-frontent - open (13: Permission denied)  
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontent), are you root?  
  
(kali@kali)-[~]  
└─$ sudo apt install nmap  
[sudo] password for kali:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
nmap is already the newest version (7.94+dfsg1-1kali1).  
nmap set to manually installed.  
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

يستخدم للحصول على مساعدة مفصلة لأمر معين: **man**:

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
└─$ man touch
```

ستظهر صفحة كاملة لشرح الأمر بالتفصيل، للخروج اضغط حرف **Q**

```
kali@kali: ~  
File Actions Edit View Help  
TOUCH(1) User Commands TOUCH(1)  
  
NAME  
touch - change file timestamps  
  
SYNOPSIS  
touch [OPTION]... FILE...  
  
DESCRIPTION  
Update the access and modification times of each FILE to the current time.  
  
A FILE argument that does not exist is created empty, unless -c or -h is supplied.  
  
A FILE argument string of - is handled specially and causes touch to change the times of the file associated with standard output.  
  
Mandatory arguments to long options are mandatory for short options too.  
  
-a change only the access time  
  
-c, --no-create do not create any files  
  
Manual page touch(1) line 1 (press h for help or q to quit)
```

ايضا يمكن الحصول على المساعدة باستخدام أمر **help** -- كما موضح ادناه

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
└─$ cat --help
Usage: cat [OPTION]... [FILE]...
Concatenate FILE(s) to standard output.

With no FILE, or when FILE is -, read standard input.

-A, --show-all          equivalent to -vET
-b, --number-nonblank   number nonempty output lines, overrides -n
-e                      equivalent to -VE
-E, --show-ends        display $ at end of each line
-n, --number            number all output lines
-s, --squeeze-blank    suppress repeated empty output lines
-t                      equivalent to -vT
-T, --show-tabs        display TAB characters as ^I
-u                      (ignored)
-v, --show-nonprinting use ^ and M- notation, except for LFD and TAB
--help                display this help and exit
--version              output version information and exit

Examples:
cat f - g  Output f's contents, then standard input, then g's contents.
cat        Copy standard input to standard output.

GNU coreutils online help: <https://www.gnu.org/software/coreutils/>
Full documentation <https://www.gnu.org/software/coreutils/cat>
or available locally via: info '(coreutils) cat invocation'
```

ifconfig: لعرض معلومات عن واجهات الشبكة وعناوين IP

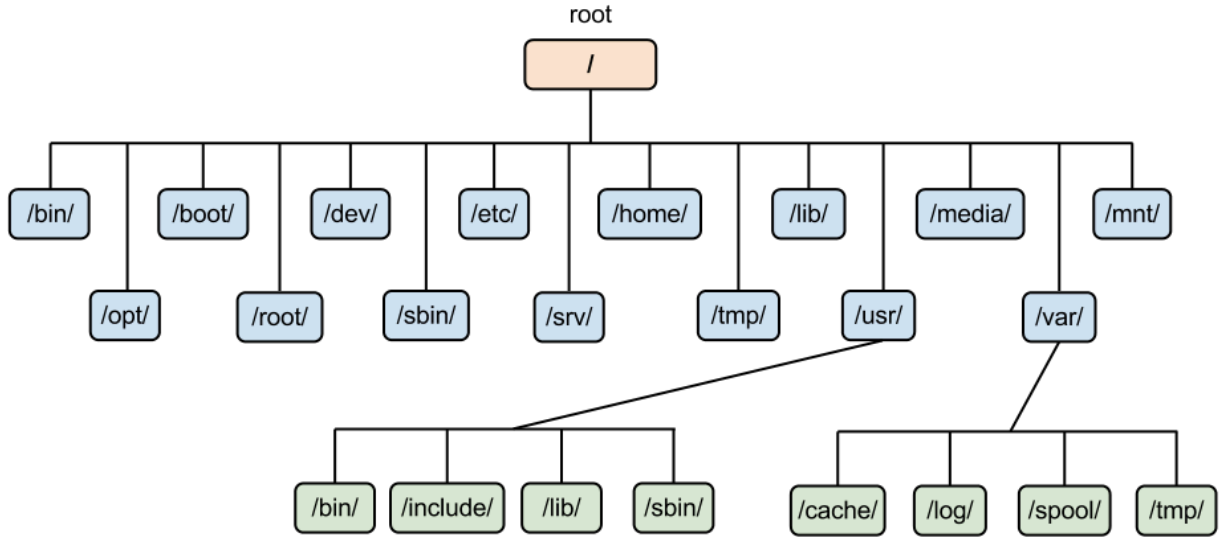
```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.11.128 netmask 255.255.255.0 broadcast 192.168.11.255
    inet6 fe80::edb6:6d87:40ae:6ca0 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:9d:59:5f txqueuelen 1000 (Ethernet)
    RX packets 232 bytes 42200 (41.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 77 bytes 22963 (22.4 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 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

ping: يستخدم لاختبار الاتصال بمضيف عبر شبكة IP

```
kali@kali: ~
File Actions Edit View Help
(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=38.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=34.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=36.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=36.4 ms
^C
— 8.8.8.8 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 34.501/36.509/38.561/1.436 ms
```

Kali Linux التسلسل الهرمي لنظام



No	Directory	Content
1	/	نظام الملفات الجذري
2	/boot	يحتوي على ملفات ثابتة وغير قابلة للمشاركة تتعلق بالتمهيد الأولي للكمبيوتر
3	/bin	يحتوي على بعض الملفات التنفيذية الهامة، مثل ls ، cp ، mount هذه الأوامر يمكن الوصول إليها من قبل جميع المستخدمين
4	/sbin	يحتوي على البرامج التي يتم تشغيلها عادة فقط من قبل مسؤول النظام
5	/lib	يحتوي على مكتبات البرامج
6	/etc	يحتوي على جميع التكوينات
7	/dev	يحتوي على جميع ملفات الجهاز على النظام
8	/tmp	يحتوي على جميع الملفات المؤقتة على النظام

9	/var	يحتوي على ملفات عابرة من أنواع مختلفة من ملفات سجل النظام وملفات التخزين المؤقت للطباعة وملفات البريد والأخبار
10	/proc	نظام ملفات افتراضي تم إنشاؤه ديناميكياً بواسطة Linux لتوفير الوصول الى أنواع معينة من معلومات الأجهزة التي لا يمكن الوصول إليها عبر /dev
11	/usr	مجلد لتخزين البرامج والملفات ذات صلة بالمستخدمين، يحتوي على ملف البرامج التنفيذية ، المكتبات وغيرها
12	/home	يحتوي هذا الدليل على بيانات المستخدم
13	/media	يحتوي على وسائط قابلة للإزالة
14	/opt	دليل اختياري تم تثبيت بعض التطبيقات عليه بشكل افتراضي مثل (oracle ,....
15	/root	الدليل الرئيسي للمستخدم الجذر

أوضاع الوصول إلى Kali Linux

Command Line interface CLI (واجهة سطر الأوامر)

الوضع الافتراضي للخادم

TTY 6 (محطة teletype) على النظام ومفيدة عندما يكون لديك وصول مادي إلى الخادم

التبديل من tty إلى آخر باستخدام زر **Alt + Ctrl + Fn**

Ctrl+Alt+F1 (tty1)

Ctrl+Alt+F4 (tty4)

Ctrl+Alt+F2 (tty2)

Ctrl+Alt+F5 (tty5)

Ctrl+Alt+F3 (tty3)

Ctrl+Alt+F6 (tty6)

عند الدخول إلى واجهة سطر الأوامر سيطلب منك ادخال Username & Password

username: **kali** & password **kali**

```
Kali GNU/Linux Rolling kali tty1
kali login: Kali
Password: Kali
```

إذا كنت في tty وتريد الانتقال إلى tty آخر، يمكنك الضغط على **Alt+Fn**

Graphical User Interface GUI (واجهة المستخدم الرسومية)



يمكن تعيينه على وضع الوصول الافتراضي إذا تم تثبيته

يحتوي على قوائم وأيقونات ورسومات

إذا كنت تريد الدخول إلى الواجهة الرسومية أو العودة إليها **Ctrl+Alt+F7**

أوامر مختلفة لإيقاف أو إعادة تشغيل النظام

init 0	إيقاف تشغيل النظام
sudo shutdown -h now	إيقاف التشغيل بزمان معين: ساعة h ، دقيقة m ، الان now
halt	إيقاف تشغيل النظام، يعمل بصلاحيات الروت Sudo
reboot	إيقاف وإعادة التشغيل
init 6	إعادة تشغيل النظام

إدارة حسابات المستخدمين والمجموعات

Root User / SuperUser	<ul style="list-style-type: none">• root ID=0• لديه الصلاحيات الكاملة• التبديل من الجذر إلى المستخدم العادي لا يتطلب كلمة مرور• التبديل من المستخدم العادي إلى الجذر يتطلب كلمة مرور (kali)• عادةً ما تكون صلاحيات الـ Root مطلوبة لتثبيت البرنامج• الدليل الرئيسي للجذر مخزن في مجلد root/
Service User / System Users	<ul style="list-style-type: none">• معرف المستخدم يبدأ من 1 إلى 49 في الإصدارات القديمة• معرف المستخدم يبدأ من 1 إلى 999 في الإصدارات الجديدة• لا توجد لديه صلاحيات على النظام• لا يسمح له بالدخول إلى النظام

<p>Normal User</p>	<ul style="list-style-type: none"> • معرف المستخدم يبدأ من 500 في الإصدارات القديمة • معرف المستخدم يبدأ من 1000 في الإصدارات الجديدة • توجد لديه صلاحيات محدودة على النظام • يسمح له بالدخول إلى النظام • التبديل إلى المستخدم الجذر يتطلب كلمة المرور (kali) • الدليل الرئيسي للمستخدم مخزن في مجلد home/ • التبديل من مستخدم عادي إلى مستخدم عادي يتطلب كلمة مرور
---------------------------	--

ما هو امر **sudo**؟ 🤔

- الجذر (**Root**) هو المستخدم الفائق ولديه القدرة على فعل أي شيء على النظام لذلك من أجل الحصول على حماية ضد الضرر المحتمل يستخدم **sudo** بدلا من **root**.
- يسمح **Sudo** للمستخدم والمجموعة بالوصول إلى الأوامر التي لا يمكنهم استخدامها عادةً.
- سيسمح **Sudo** للمستخدم بالحصول على امتيازات المسؤول دون تسجيل الدخول ك **.Root**.
- من أجل تزويد المستخدم بصلاحيات **sudo** يجب إضافة اسمه إلى ملف **sudoers**.
- هذا الملف مهم جدًا ولا يجب تحريره مباشرةً باستخدام محرر النصوص
- إذا تم تحرير ملف **sudoers** بشكل غير صحيح، فقد يؤدي ذلك إلى منع الوصول إلى النظام.

خطوات هامة يجب القيام بها عند تثبيت Kali Linux

1- تحديث النظام باستخدام الأوامر:

`sudo apt update`

`sudo apt upgrade`

2- تثبيت أدوات الأمان يحتوي: **Kali Linux** على العديد من أدوات الأمان واختبار الاختراق مُسبقة التثبيت. يمكنك استكشاف واستخدام هذه الأدوات لأغراض الاختبار والاستفادة منها، مثل **Metasploit Framework , Wireshark , Nmap**.

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)~  
└─$ sudo apt install nmap  
[sudo] password for kali:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
nmap is already the newest version (7.94+dfsg1-1kali1).  
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.  
  
(kali@kali)~  
└─$ sudo apt install wireshark  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
wireshark is already the newest version (4.0.7-1).  
wireshark set to manually installed.  
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

3- تكوين الشبكة: تأكد من تكوين الشبكة بشكل صحيح والوصول إلى الإنترنت إذا كنت بحاجة إلى تحديثات أو تنزيل أدوات إضافية،

استخدم أمر **ifconfig** لعرض الواجهات المتاحة:

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)~  
└─$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.0.229 netmask 255.255.255.0 broadcast 192.168.0.255  
    inet6 fe80::20c:29ff:fe00:0000 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:00:00:00 txqueuelen 1000 (Ethernet)  
    RX packets 519 bytes 86799 (84.7 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 215 bytes 40902 (39.9 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 4 bytes 240 (240.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4 bytes 240 (240.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)~
```

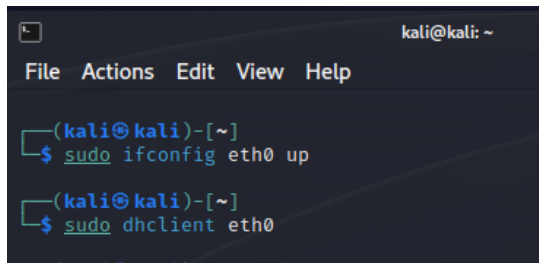
ابحث عن واجهة الشبكة التي ترغب في تكوينها، عادةً تكون مسماة بشكل مشابه لـ "eth0" للاتصال بالشبكة السلكية أو "wlan0" للاتصال بالشبكة اللاسلكية.

تكوين الشبكة السلكية (Ethernet):

استخدام الأمر التالي لتفعيل الواجهة والحصول على عنوان IP بشكل تلقائي من خلال DHCP:

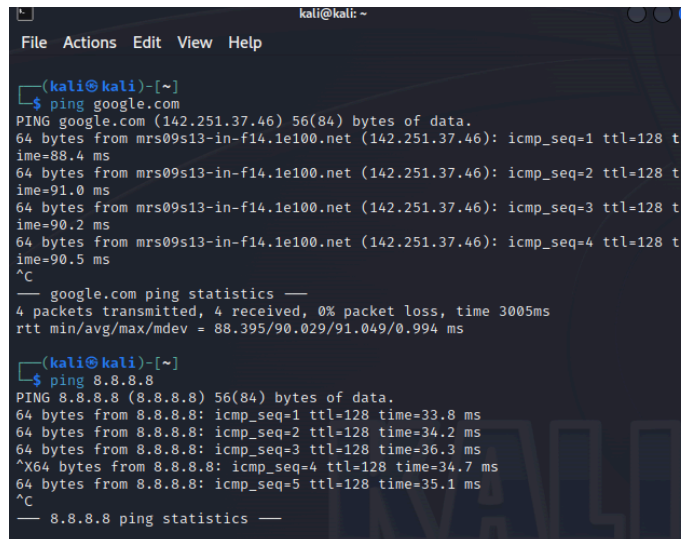
```
sudo ifconfig eth0 up
```

```
sudo dhclient eth0
```



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
└─$ sudo ifconfig eth0 up  
(kali@kali)-[~]  
└─$ sudo dhclient eth0
```

اختبار الاتصال: للتحقق من أنك متصل بالإنترنت بنجاح، يمكنك استخدام أمر "ping" مع عنوان IP أو اسم مضيف معروف. على سبيل المثال:



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
└─$ ping google.com  
PING google.com (142.251.37.46) 56(84) bytes of data.  
64 bytes from mrs09s13-in-f14.1e100.net (142.251.37.46): icmp_seq=1 ttl=128 time=88.4 ms  
64 bytes from mrs09s13-in-f14.1e100.net (142.251.37.46): icmp_seq=2 ttl=128 time=91.0 ms  
64 bytes from mrs09s13-in-f14.1e100.net (142.251.37.46): icmp_seq=3 ttl=128 time=90.2 ms  
64 bytes from mrs09s13-in-f14.1e100.net (142.251.37.46): icmp_seq=4 ttl=128 time=90.5 ms  
^C  
— google.com ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3005ms  
rtt min/avg/max/mdev = 88.395/90.029/91.049/0.994 ms  
(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=33.8 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=34.2 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=36.3 ms  
^X64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=34.7 ms  
64 bytes from 8.8.8.8: icmp_seq=5 ttl=128 time=35.1 ms  
^C  
— 8.8.8.8 ping statistics —
```

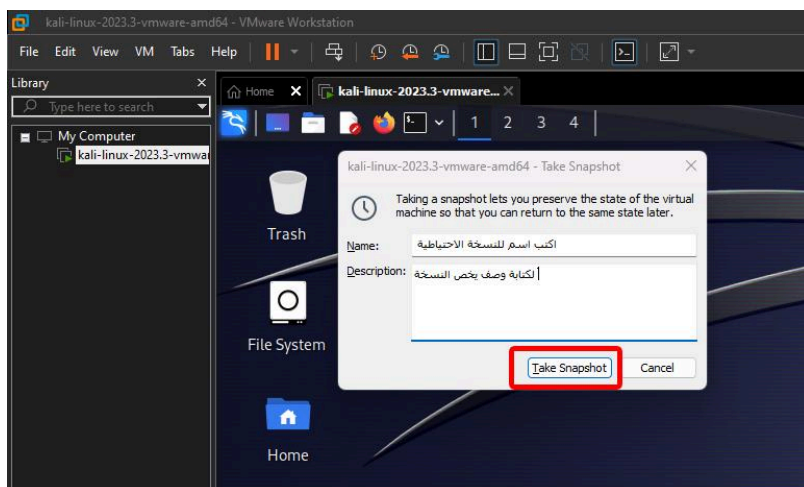
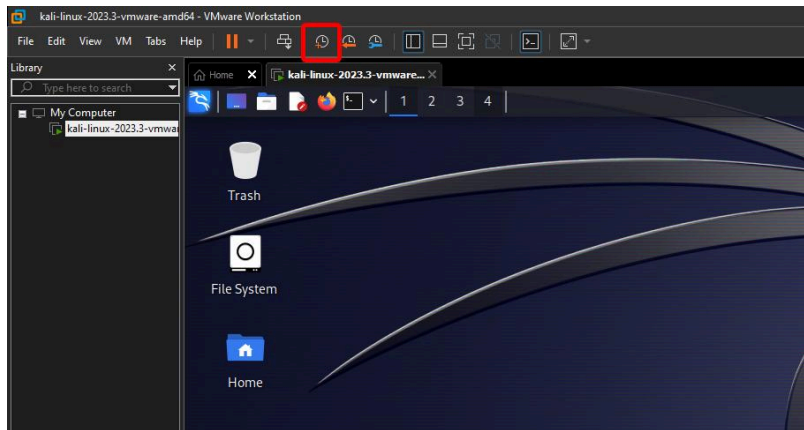
4- القيام بالنسخ الاحتياطي: قم بعمل نسخ احتياطي للبيانات الهامة والإعدادات قبل البدء في تكوين النظام، يمكنك استخدام "dd" لنسخ القرص الصلب بالكامل إلى ملف صورة أو قرص آخر. تأكد من توجيه النسخ الاحتياطي إلى وجهة آمنة.

لاستخدام "dd" لنسخ القرص:

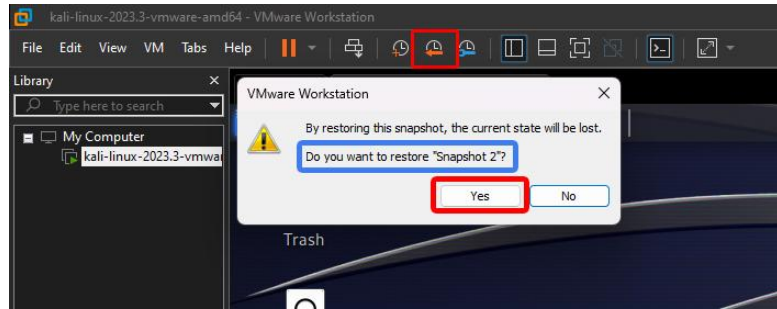
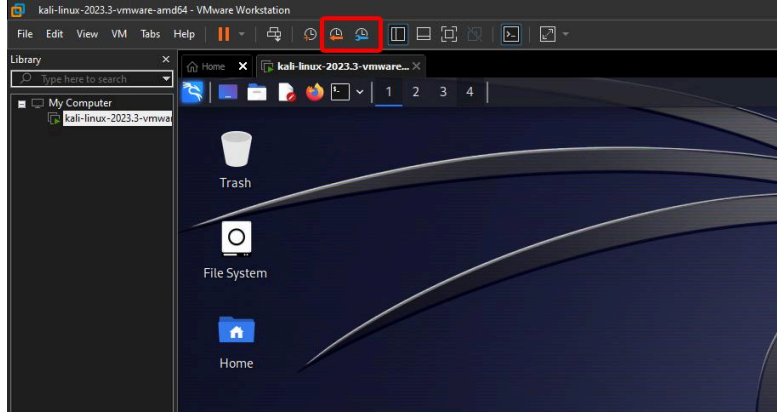
sudo dd if=/dev/sda of = اسم الملف للحفظ النسخة bs=4M

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
└─$ sudo dd if=/dev/sda of=test bs=4M
```

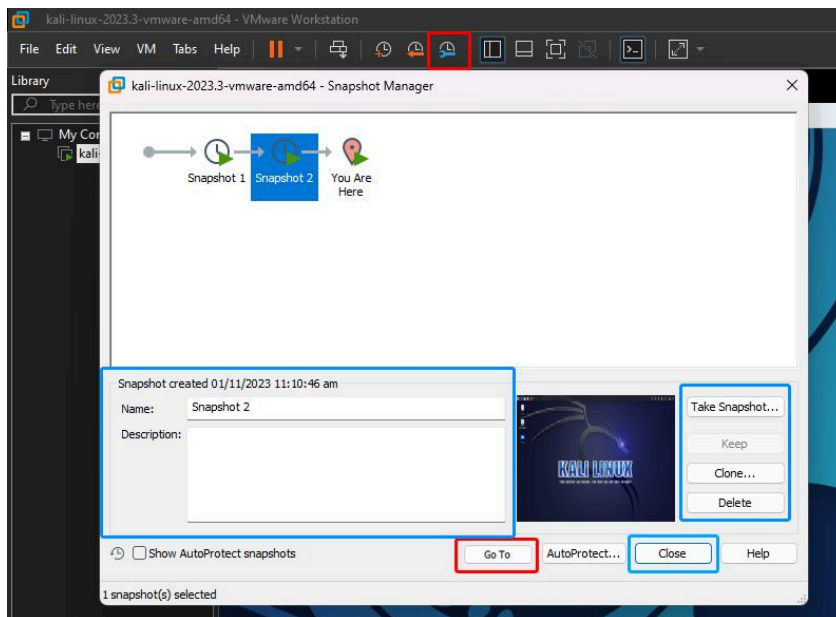
ايضاً يمكنك عمل نسخ احتياطي للنظام من برنامج **Workstation Pro** باستخدام ميزة **snapshot**:



للرجوع الى النسخة الاحتياطية السابقة:



الخيار أدناه لتعديل اي نسخة احتياطية تم اخذها سابقاً او حذفها، او الدخول اليها



5- تعلم وتحسين مهارات الاستخدام: **Kali Linux** تتيح لك الوصول إلى مجموعة واسعة من أدوات الأمان واختبار الاختراق. قم بتعلم كيفية استخدامها بشكل فعال وتحسين مهاراتك.

6- تشغيل التحديثات التلقائية: يُفضل تكوين نظام التحديث التلقائي لضمان حصولك على التحديثات الأمنية الأخيرة.

7- تكوين جدار الحماية (Firewall): قم بتكوين جدار الحماية (firewall) لتقييد الوصول إلى النظام وحمايته من الهجمات.

تكوين جدار حماية قم بتثبيت الأمر **UFW**:

sudo apt install ufw

```
kali@kali: ~  
File Actions Edit View Help  
~(kali@kali)-[~]  
└─$ sudo apt install ufw  
[sudo] password for kali:  
Reading package lists ... Done  
Building dependency tree ... Done  
Reading state information... Done  
ufw is already the newest version (0.36.2-1).  
The following packages were automatically installed and are no longer require  
d:  
  gcc-12-base libarmadillo11 libcbor0.8 libcodec2-1.1 libcurl3-nss  
  libgcc-12-dev libgumbo1 libgupnp-igd-1.0-4 libjim0.81 libnfs13  
  libobjc-12-dev libstdc++-12-dev libtexluaajit2 libutf8proc2 libvpx7  
  nss-plugin-pem python3-jdcal python3-pyminifier  
Use 'sudo apt autoremove' to remove them.  
0 upgraded, 0 newly installed, 0 to remove and 7 not upgraded.
```

بعد التثبيت، قم بتفعيل **UFW** باستخدام الأمر:

sudo ufw enable

```
kali@kali: ~  
File Actions Edit View Help  
~(kali@kali)-[~]  
└─$ sudo ufw enable  
Firewall is active and enabled on system startup
```

يمكنك تكوين قواعد الجدار وتحديد الخدمات والمنافذ التي ترغب في السماح بالوصول إليها ومنع الوصول إليها. على سبيل المثال، للسماح بالوصول إلى SSH (المنفذ 22):

sudo ufw allow 22/tcp

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
└─$ sudo ufw allow 22/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)
```

لمنع الوصول إلى منفذ معين (منفذ 8080 كمثال):

sudo ufw deny 8080/tcp

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
└─$ sudo ufw deny 8080/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)
```

بعد تكوين قواعد الجدار، قم بتفعيله باستخدام الأمر: **sudo ufw enable**

يمكنك التحقق من حالة **UFW** باستخدام أمر:

sudo ufw status

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
└─$ sudo ufw status
Status: active

To Action From
--
22/tcp ALLOW Anywhere
8080/tcp DENY Anywhere
22/tcp (v6) ALLOW Anywhere (v6)
8080/tcp (v6) DENY Anywhere (v6)
```

إذا كنت ترغب في تشغيل **UFW** عند بدء تشغيل النظام، فيمكنك تكوين ذلك باستخدام أمر:

sudo systemctl enable ufw

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
└─$ sudo ufw status
Status: active

To Action From
--
22/tcp ALLOW Anywhere
8080/tcp DENY Anywhere
22/tcp (v6) ALLOW Anywhere (v6)
8080/tcp (v6) DENY Anywhere (v6)
```

-8 تحديث كلمة المرور الافتراضية: تأكد من تغيير كلمة المرور الافتراضية للمستخدم الجذر (**root**) وأي مستخدمين آخرين إذا كانوا موجودين.

استخدم الأمر "**passwd**" مع اسم المستخدم لتغيير كلمة المرور. أدخل الأمر التالي واستبدل "**username**" بالاسم الذي ترغب في تغيير كلمة مروره:

sudo passwd username

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
└─$ sudo passwd kali
[sudo] password for kali:
New password:
Retype new password:
passwd: password updated successfully
```

أهم أدوات Kali Linux

اسم الأداة	الوظيفة	الشعار
Nmap	أداة مسح الشبكة التي تستخدم لفحص الشبكات واكتشاف الأجهزة والخدمات المتاحة عليها	
Wireshark	برنامج مراقبة حركة البيانات عبر الشبكة، يمكن استخدامه لتحليل حركة الشبكة واكتشاف الهجمات	
Metasploit Framework	منصة قوية لاستغلال الثغرات واختبار الأمان، تمكن محترفي الأمان من اختبار الأمان والاختراق	
Burp Suite	أداة اختبار الأمان التي تستخدم لاكتشاف ثغرات الويب واختبار الأمان في تطبيقات الويب	
Hydra	أداة لاختبار قوة كلمات المرور، يمكن استخدامها لمحاولة اختراق حسابات بكلمات مرور ضعيفة	
John the Ripper	أداة قوية لاختبار قوة كلمات المرور، تعتمد على هجمات تخمين كلمة المرور	

Sqlmap	أداة تستخدم لاكتشاف واستغلال ثغرات قواعد البيانات SQL	
Nikto	أداة اختبار الأمان تستخدم لفحص تطبيقات الويب واكتشاف الثغرات الشائعة	
Hashcat	أداة لاختبار قوة كلمات المرور تستخدم لكسر واستنباط كلمات المرور المشفرة.	
Maltego	أداة تحليل الأمان تستخدم لجمع وتحليل المعلومات على الإنترنت	

لتثبيت إحدى الأدوات أعلاه استخدام أمر:

اسم الأداة = `sudo apt install`

مثال:

```

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
└─$ sudo apt install sqlmap
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
sqlmap is already the newest version (1.7.10-1).
sqlmap set to manually installed.
The following packages were automatically installed and are no longer require
d:
 gcc-12-base libarmadillo11 libcbor0.8 libcodecs2-1.1 libcurl3-nss
 libgcc-12-dev libgumbo1 libgupnp-igd-1.0-4 libjim0.81 libnfs13
 libobjc-12-dev libstdc++-12-dev libtexluaajit2 libutf8proc2 libvpx7
 nss-plugin-pem python3-jdcal python3-pyminifier
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 7 not upgraded.

```


للمزيد من التفاصيل حول أمر معين استخدم **help --**

useradd --help
usermod --help
userdel --help
passwd --help

المجموعات

groupadd	إنشاء مجموعة جديدة
groupmod	تعديل المجموعة
gpasswd	ضبط او تعيين كلمة مرور
groupdel	حذف المجموعة

للمزيد من التفاصيل حول أمر معين استخدم **help --**

groupadd--help
groupmod--help
gpasswd--help
groupdel--help

المعلومات المخزنة حول المستخدمين و المجموعات

يجب أن تكون مستخدم رئيسي (**root**) لقراءة الملف، او استخدم أمر **sudo**

لمعرفة المستخدمين من خلال:

sudo cat /etc/passwd

```
kali@kali: ~
File Actions Edit View Help
nm-openconnect:x:115:122:NetworkManager OpenConnect plugin,,:/var/lib/NetworkManager:/usr/sbin/nologin
mysql:x:116:124:MySQL Server,,:/nonexistent:/bin/false
stunnel4:x:995:995:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin
_rpc:x:117:65534::/run/rpcbind:/usr/sbin/nologin
geoclue:x:118:126::/var/lib/geoclue:/usr/sbin/nologin
Debian-snmpp:x:119:127::/var/lib/snmp:/bin/false
sslh:x:120:128::/nonexistent:/usr/sbin/nologin
ntpsec:x:121:131::/nonexistent:/usr/sbin/nologin
redsocks:x:122:132::/var/run/redsocks:/usr/sbin/nologin
rwhod:x:123:65534::/var/spool/rwho:/usr/sbin/nologin
_gophish:x:124:134::/var/lib/gophish:/usr/sbin/nologin
iodine:x:125:65534::/run/iodine:/usr/sbin/nologin
miredo:x:126:65534::/var/run/miredo:/usr/sbin/nologin
statd:x:127:65534::/var/lib/nfs:/usr/sbin/nologin
redis:x:128:135::/var/lib/redis:/usr/sbin/nologin
postgres:x:129:136:PostgreSQL administrator,,:/var/lib/postgresql:/bin/bash
mosquitto:x:130:138::/var/lib/mosquitto:/usr/sbin/nologin
inetsim:x:131:139::/var/lib/inetsim:/usr/sbin/nologin
_gvm:x:132:141::/var/lib/openvas:/usr/sbin/nologin
kali:x:1000:1000:,,:/home/kali:/usr/bin/zsh
test1:x:1001:1001::/home/test1:/bin/sh
test:x:1002:1002::/home/test:/bin/sh

(kali@kali)-[~]
```

اسم المستخدم	معرف المستخدم	كلمة المرور	معرف المجموعة	وصف المستخدم	ملف المستخدم	نوع Shell
test	1002	xxxxx	1002	مستخدم عادي	/home/user1	/bin/bash

sudo cat /etc/shadow

```
kali@kali: ~
File Actions Edit View Help
nm-openvpn:!:19590:!:19590:!:19590:
nm-openconnect:!:19590:!:19590:!:19590:
mysql:!:19590:!:19590:!:19590:
stunnel4:!*:19590:!:19590:!:19590:
_rpc:!:19590:!:19590:!:19590:
geoclue:!:19590:!:19590:!:19590:
Debian-snmpp:!:19590:!:19590:!:19590:
sslh:!:19590:!:19590:!:19590:
ntpsec:!:19590:!:19590:!:19590:
redsocks:!:19590:!:19590:!:19590:
rwhod:!:19590:!:19590:!:19590:
_gophish:!:19590:!:19590:!:19590:
iodine:!:19590:!:19590:!:19590:
miredo:!:19590:!:19590:!:19590:
statd:!:19590:!:19590:!:19590:
redis:!:19590:!:19590:!:19590:
postgres:!:19590:!:19590:!:19590:
mosquitto:!:19590:!:19590:!:19590:
inetsim:!:19590:!:19590:!:19590:
_gvm:!:19590:!:19590:!:19590:
kali:$y$j9T$hVUcCzQozwQh.2JyVrs.$T0FS1BRacGSTCGLdig/Ji2CbWc3bLVV8Ym1wEPDcIw1:19590:0:99999:7::
test1:!:19660:0:99999:7::
test:!:19660:0:99999:7::

(kali@kali)-[~]
```

لمعرفة المجموعات من خلال:

sudo cat /etc/group

```
kali@kali: ~  
File Actions Edit View Help  
mysql:x:124:  
rdma:x:125:  
stunnel4:x:995:stunnel4  
geoclue:x:126:  
Debian-snmpp:x:127:  
sslh:x:128:  
ssl-cert:x:129:postgres  
i2c:x:130:  
ntpsec:x:131:  
redsocks:x:132:  
kismet:x:133:  
_gophish:x:134:  
redis:x:135:_gvm  
postgres:x:136:  
plocate:x:137:  
mosquitto:x:138:  
smbshare:x:994:  
inetsim:x:139:  
wireshark:x:140:kali  
_gvm:x:141:  
kali:x:1000:  
kaboxer:x:142:kali  
test1:x:1001:  
test:x:1002:
```

اسم المجموعة	كلمة مرور المجموعة	معرف المجموعة	الأعضاء
test	xxxxx	1002	test , test1

sudo cat /etc/gshadow

```
kali@kali: ~  
File Actions Edit View Help  
mysql:!:!  
rdma:!:!  
stunnel4:!*::stunnel4  
geoclue:!:!  
Debian-snmpp:!:!  
sslh:!:!  
ssl-cert:!:!:postgres  
i2c:!:!  
ntpsec:!:!  
redsocks:!:!  
kismet:!:!  
_gophish:!:!  
redis:!:!:_gvm  
postgres:!:!  
plocate:!:!  
mosquitto:!:!  
smbshare:!:!  
inetsim:!:!  
wireshark:!:!:kali  
_gvm:!:!  
kali:!:!  
kaboxer:!:!:kali  
test1:!:!  
test:!:!
```

أنواع الملفات المختلفة في لينكس

نوع الملف	الرمز
Normal File	-
Normal Directory	d
Hard Link	-
Soft Link	l
Character Device	c
Block Device	b
Socket File	s

إذن	ملفات	الدلائل
Read	عرض محتوى الملف	قائمة الملفات في الدليل
Write	عرض وتحرير وحذف محتوى الملف	إضافة أو حذف الملفات الموجودة على الدليل أو حذف الدليل أو تعديله
Execute	تشغيل الملف أو تنفيذه	يمكنك عمل (ls-l) أو (cd)

تعديل الأذونات

الطريقة الرمزية	الطريقة العددية
<ul style="list-style-type: none"> • user (u) • group (g) • others (o) • all (a) • mean add (+) • means remove (-) • means Set (=) <p>يستخدم أمر <code>chmod</code> لتعديل الأذونات على الملفات أو المجلدات. يمكن تعديل إذن واحد أو أكثر في نفس الوقت.</p>	<ul style="list-style-type: none"> • Read = 4 • Write = 2 • Execute = 1 • Total permission = 7 <p>يستخدم أمر <code>chmod 664 file 1</code> لتعديل إذن الملف.</p>

أوامر Kali Linux

/	الأمر	الوصف
1	useradd	يستخدم لإنشاء حساب مستخدم جديد
2	usermod	يستخدم لتعديل خصائص حساب المستخدم
3	userdel	يستخدم لحذف حساب المستخدم
4	passwd	يستخدم لتغيير كلمة المرور لحساب المستخدم
5	groupadd	يستخدم لإنشاء مجموعة مستخدم جديدة

6	groupmod	يستخدم لتعديل خصائص المجموعات الموجودة في النظام
7	groupdel	يستخدم لحذف مجموعة مستخدم
8	gpasswd	تعيين أو تغيير كلمة مرور المجموعة
9	id	يستخدم لعرض معلومات حول المستخدم
10	touch	يستخدم لإنشاء ملف جديد فارغ أو تحديث وقته
11	mkdir	يستخدم لإنشاء مجلد جديد أو أكثر
12	cd	يستخدم لتغيير المجلد الحالي (المجلد الذي تتواجد فيه)
13	chmod	يستخدم لتغيير صلاحيات الوصول للملفات والمجلدات
14	chattr	يستخدم لتعيين أو إزالة سمات خاصة على الملفات والمجلدات
15	lsattr	يستخدم لعرض السمات للملفات والمجلدات
16	chown	يستخدم لتغيير مالك الملفات والمجلدات
17	ls	يستخدم لعرض قائمة الملفات والمجلدات في المجلد الحالي
18	groups	يستخدم لعرض المجموعات التي ينتمي إليها المستخدم
19	fdisk	يستخدم لإدارة أقراص التخزين (لإنشاء وتعديل وحذف الأقسام على الأقراص)
20	mkfs	يستخدم لإنشاء نظام ملفات على جهاز تخزين مثل الأقراص
21	df (disk free)	يستخدم لعرض معلومات حول المساحة المستخدمة والمساحة المتاحة
22	mount	يستخدم لربط (توصيل) نظام ملفات معين بنظام الملفات (root)
23	umount	يستخدم لفصل (فصل توصيل) أقسام الأقراص أو الأجهزة القابلة للإزالة
24	e2label	يستخدم لتعيين أو تغيير العلامة لنظام الملفات (label)
25	blkid (block ID)	يستخدم لعرض معلومات حول أجهزة التخزين والأقسام (الأقراص) المتصلة
26	ls -il	يستخدم لعرض معلومات مفصلة حول الملفات والمجلدات في الدليل الحالي
27	df -ih	يستخدم لعرض معلومات حول توزيع مساحة التخزين على الأقراص

28	e2fsck	يستخدم لفحص وإصلاح أخطاء في نظام الملفات
29	dumpe2fs	تستخدم لاستخراج معلومات تفصيلية حول نظام الملفات
30	tune2fs	يستخدم لتعديل معلومات وإعدادات نظام الملفات
31	mkswap	يستخدم لإنشاء ملف تبادل أو تهيئة جزء من القرص الصلب
32	swapon	يستخدم لتنشيط ملفات التبادل أو أقسام التبادل
33	swapon -a	يستخدم لتنشيط جميع ملفات التبادل المُعرفة (swap files)
34	cp (copy)	يستخدم لنسخ ملفات ومجلدات من موقع إلى موقع آخر
35	mv (Move)	يستخدم لنقل ملفات ومجلدات من مكان إلى مكان آخر
36	rm (Remove)	يستخدم لحذف ملفات أو مجلدات من نظام الملفات
37	gzip	يستخدم لضغط الملفات وإنشاء ملفات مضغوطة
38	gunzip	يستخدم لفك ضغط ملفات المضغوطة GZIP
39	bzip2	يستخدم لضغط وفك ضغط الملفات باستخدام الخوارزمية Bzip2
40	bunzip2	يستخدم لفك ضغط الملفات المضغوطة باستخدام الخوارزمية Bzip2
41	tar	يستخدم لإنشاء وإدارة ملفات الأرشيف والمجلدات
42	find	يستخدم للبحث عن ملفات ومجلدات داخل النظام
43	locate	يستخدم للعثور عن ملفات ومجلدات داخل النظام
44	whereis	يستخدم للبحث عن المواقع (المسارات) الرئيسية
45	which	يستخدم للعثور على المسار (المكان) الذي يحتوي على ملف تنفيذي معين لبرنامج أو أمر محدد
46	head	يستخدم لعرض الأسطر الأولى من ملف نصي
47	tail	يستخدم لعرض الأسطر الأخيرة من ملف نصي
48	less	يستخدم لعرض محتوى ملف نصي بطريقة يمكنك التصفح والتمرير خلفياً دون الحاجة لفتح الملف بمحرر نصي

49	cat	يستخدم لعرض محتوى ملف نصي على الشاشة
50	ps	يستخدم لعرض معلومات عن العمليات (البرامج)
51	ps a	يستخدم لعرض معلومات عن العمليات (العمليات الجارية)
52	ps aux	يستخدم لعرض معلومات مفصلة عن جميع العمليات
53	pstree	يستخدم لعرض هيكل العمليات
54	ps -ef	يستخدم لعرض معلومات مفصلة حول جميع العمليات (العمليات الجارية) في النظام
55	pgrep	يستخدم للبحث عن عمليات
56	kill	يستخدم لإنهاء (إيقاف) العمليات
57	nice	يستخدم لتغيير أولوية تنفيذ العمليات
58	jobs	يستخدم لعرض وإدارة الأعمال
59	fg	يستخدم لجلب عملية من الخلفية إلى الأمامية
60	bg	يستخدم لتشغيل العمليات في الخلفية أو لإعادة تنفيذ العمليات في الخلفية
61	runlevel	يستخدم لعرض مستوى التشغيل
62	telinit	يستخدم لتغيير مستوى التشغيل
63	chkconfig	يستخدم لإدارة خدمات النظام وتكوينها لتشغيلها تلقائيًا عند بدء تشغيل النظام

اختصارات Kali Linux (لوحة المفاتيح)

يمكنك استخدام العديد من الاختصارات في لوحة التحكم (Terminal) لتسهيل تنفيذ الأوامر وزيادة الإنتاجية. إليك بعض الاختصارات الشائعة في لوحة المفاتيح:

الاختصار	الوظيفة
Tab	استكمال التعبئة التلقائية (Auto Complete) للملفات والأوامر
Ctrl + C	لإلغاء تشغيل الأمر الجاري أو البرنامج
Ctrl + Z	لوقف تشغيل الأمر مؤقتًا ووضعه في الخلفية. يمكن استئنافه باستخدام "fg"
Ctrl + D	للخروج من الجلسة الحالية أو إغلاق النافذة.
Ctrl + L	لمسح الشاشة وتنظيفها
Ctrl + A	للانتقال إلى بداية السطر الحالي
Ctrl + E	للانتقال إلى نهاية السطر الحالي
Ctrl + U	لحذف النص من موضع المؤشر إلى بداية السطر
Ctrl + K	لحذف النص من موضع المؤشر إلى نهاية السطر
Ctrl + R	للبحث عن أوامر سابقة باستخدام محرك البحث
Up Arrow / Down Arrow	للتنقل بين الأوامر السابقة واللاحقة في سجل الأوامر
Ctrl + Shift + T	لفتح نافذة تحكم إضافية
Ctrl + Shift + W	لإغلاق نافذة تحكم حالية
Ctrl + Alt + T	لفتح نافذة تحكم جديدة
Ctrl + Alt + F1 إلى F6	لتبديل بين نوافذ (TTY)

النهاية

في ختام هذا الشرح عن نظام التشغيل **Kali Linux** يمكن القول إن **kali Linux** يمثل أداة قوية وضرورية لمجتمع الأمان واختبار الاختراق، ويتيح للمحترفين والمطورين وأي شخص مهتم بأمن المعلومات إمكانية الوصول إلى مجموعة كبيرة من الأدوات والموارد المخصصة لاختبار الأمان والتحقق من الثغرات. **Kali Linux** ليس مجرد نظام تشغيل، بل هو أيضًا مجتمع نشط من المطورين ومحترفي أمان المعلومات.

● تنويه ●

أذكر أن استخدام **Kali Linux** يجب أن:

- يكون دائمًا قانونيًا وأخلاقيًا.
- يجب على المستخدمين الامتثال للقوانين والأنظمة المعمول بها في منطقتهم والالتزام بأعلى معايير الأخلاق في استخدامه.
- يجب على المستخدمين عدم انتهاك خصوصية الأفراد أو المؤسسات دون إذن صريح.
- يجب الحصول على إذن من مالك الموقع أو النظام الذي يتم اختباره.
- في حال اكتشاف أي ثغرات أمنية خلال عمليات الاختبار، يجب على المستخدمين الإبلاغ عنها بشكل مسؤول إلى مالك الموقع أو المؤسسة المعنية دون نشر المعلومات بشكل علني.

وفي نهاية الختام أرجو أن هذا الشرح قد أوفى بما قد خطر على عقلي، وما تم استخلاصه من معلومات ومحتوى يخص هذا المجال، أرجوا أن يستفيد كل من يهيمه هذا الموضوع بهذا المقال.

قال نبينا ﷺ { أفضل الصدقة أن يتعلم المرء علما ثم يعلمه أخاه المسلم }.