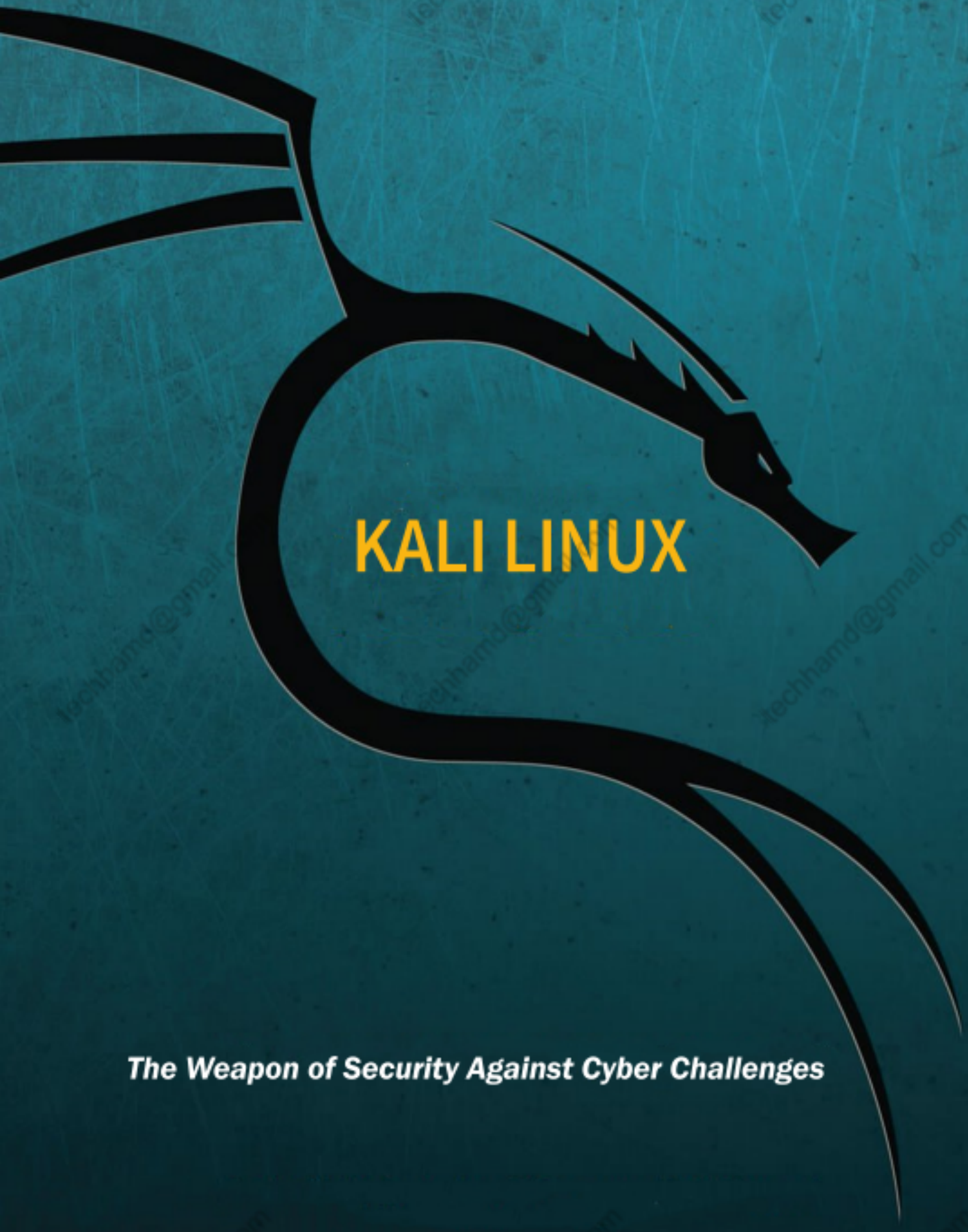


KALI LINUX

The Weapon of Security Against Cyber Challenges

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

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

ومن منطلق حبّي لنشر الفائدة، أشارك ما أتعلمه من أدوات، تطبيقات، ومصادر مفيدة — لعلها تكون عونًا 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 التعلم.

ويكفيني شرفًا أن أتمثل بقول النبي ﷺ:

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

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

📩 **للتواصل عبر البريد:**

techhamd@gmail.com

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

t.me/TechHamd

الفهرس

بسـم الله الـرحمـن الرحيـم

الحمد لله وبعد:

في عصر التكنولوجيا الحديثة، حيث أصبحت الشبكات والأنظمة الرقمية جزءً أساسيًا 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.

سـ / 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 الاخرى.

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 تثبيتة على مجموعة متنوعة من الأجهزة بما في ذلك الكمبيوترات المكتبية وأجهزة الكمبيوتر المحمول واجهزة Raspberry PI.

مفتوح المصدر:

متاح كتوزيعة مفتوحة 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 الأماني:

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.

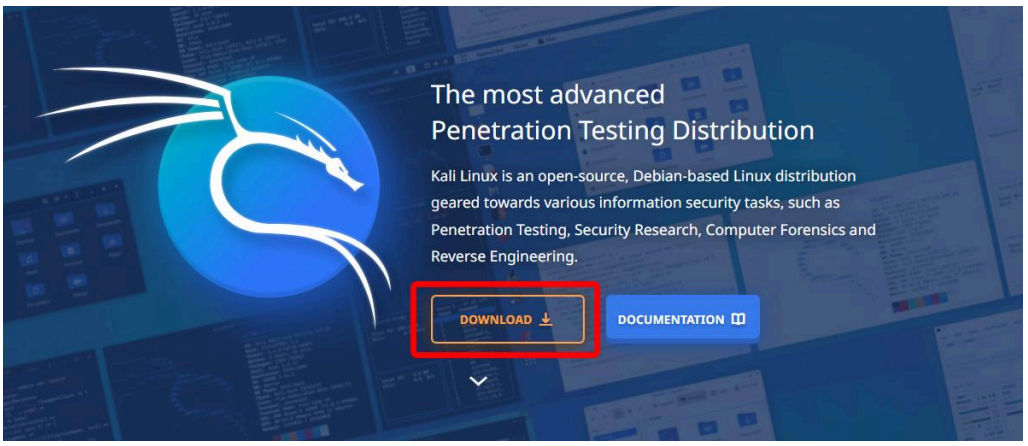
تعليم الأمن السيبراني:

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

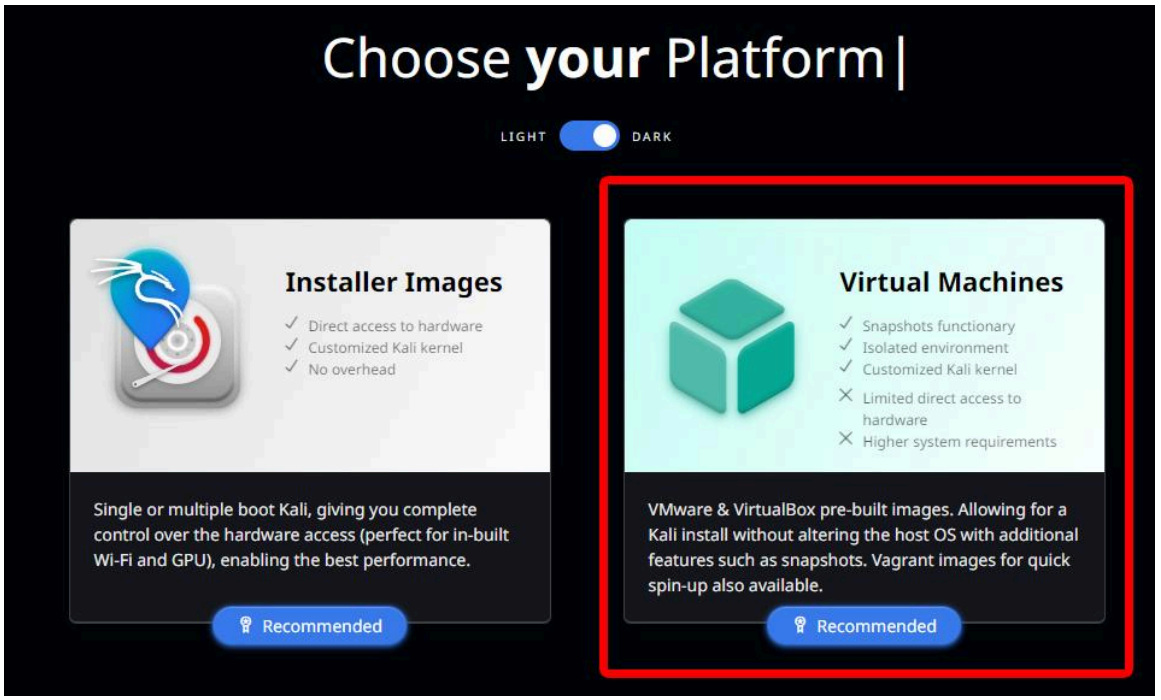
طريقة تنصيب Kali Linux على VMware Workstation

1- الدخول الى الموقع الخاص بـ kali Linux https://www.kali.org/

ثم الضغط على DOWNLOAD



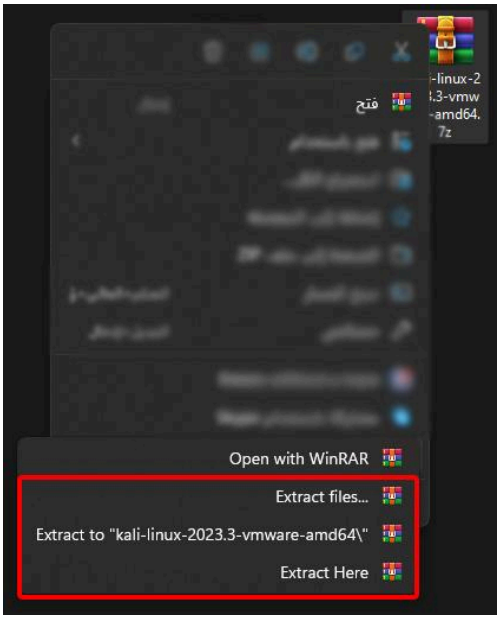
ثم اختيار Virtual Machines

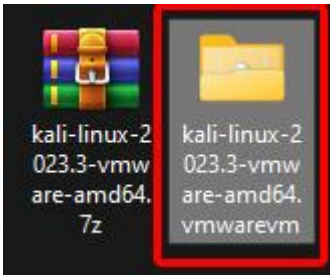


اختار نوع وحدة الجهاز الخاص بك 32 - 64 bit ثم قم باختيار VMware

يمكنك ايضاً اختيار برامج افتراضية مماثلة لـ VMware كالـ VirtualBox - Hyper - QWMU

بعد انتهاء التحميل استخراج الملف

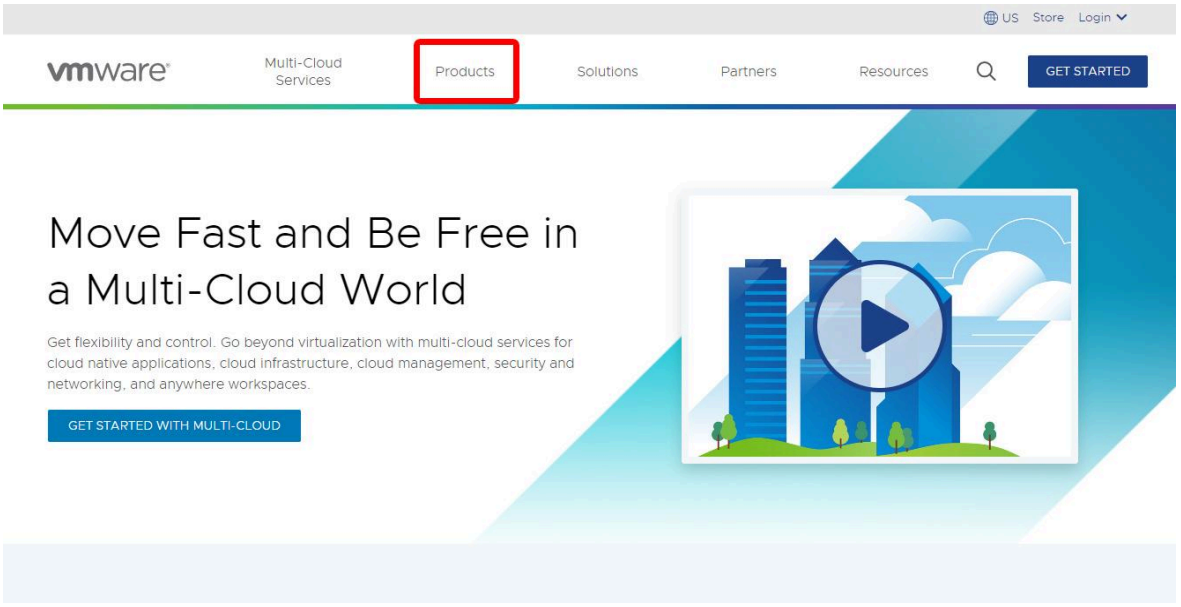




2- تحميل برنامج VMware Workstation

الدخول الى الموقع https://www.vmware.com/

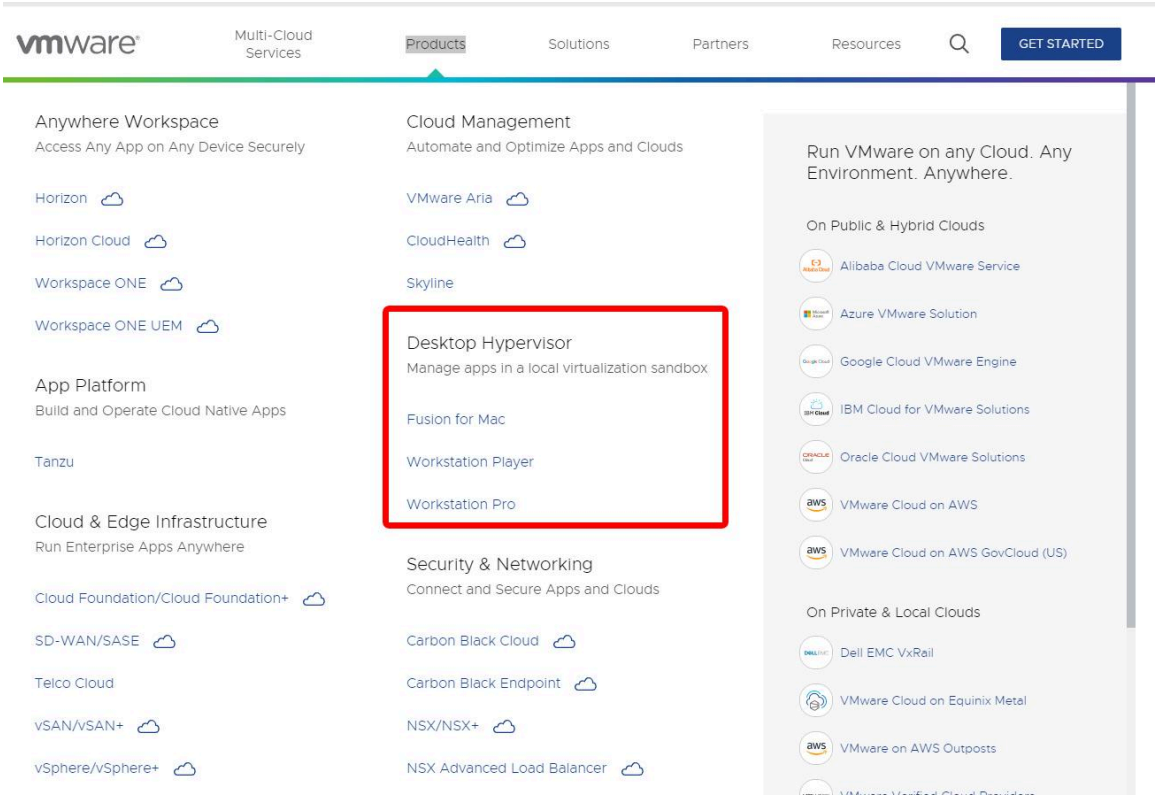
ثم الانتقال إلى Products

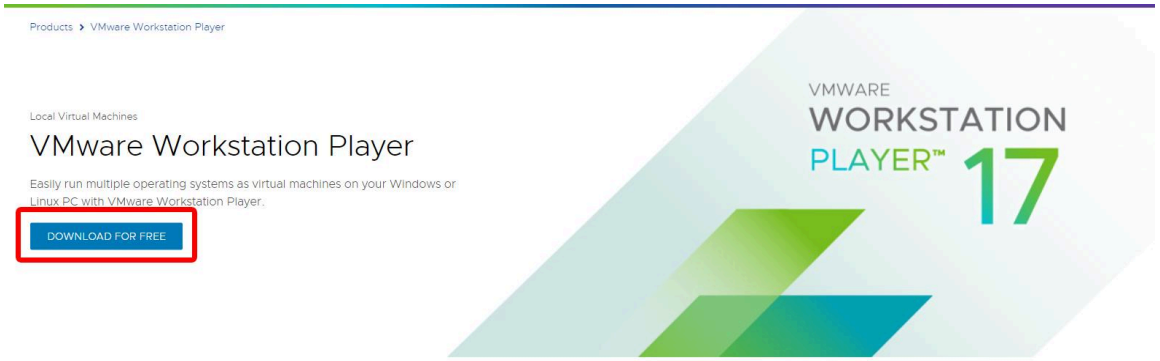


يتوفر vmware بنسختين:

مجانية باسم Workstation Player

ومدفوعة باسم Workstation Pro



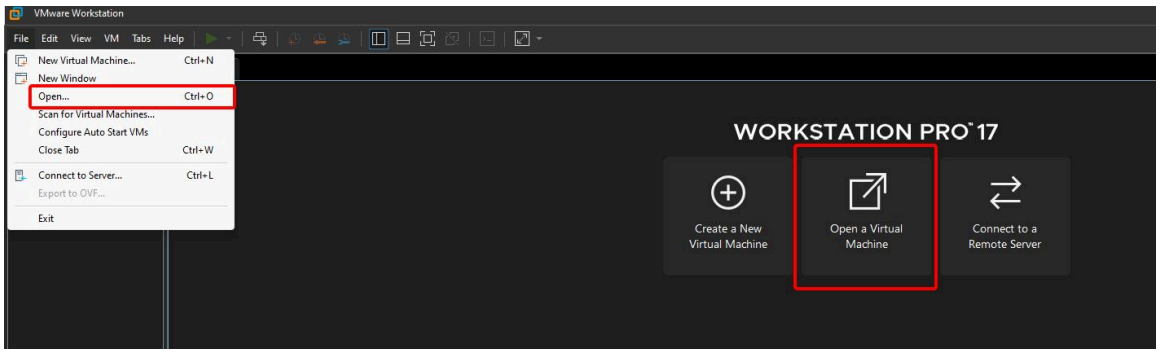


سـ/ ما الفرق بين النسخة المجانية والمدفوعة ؟

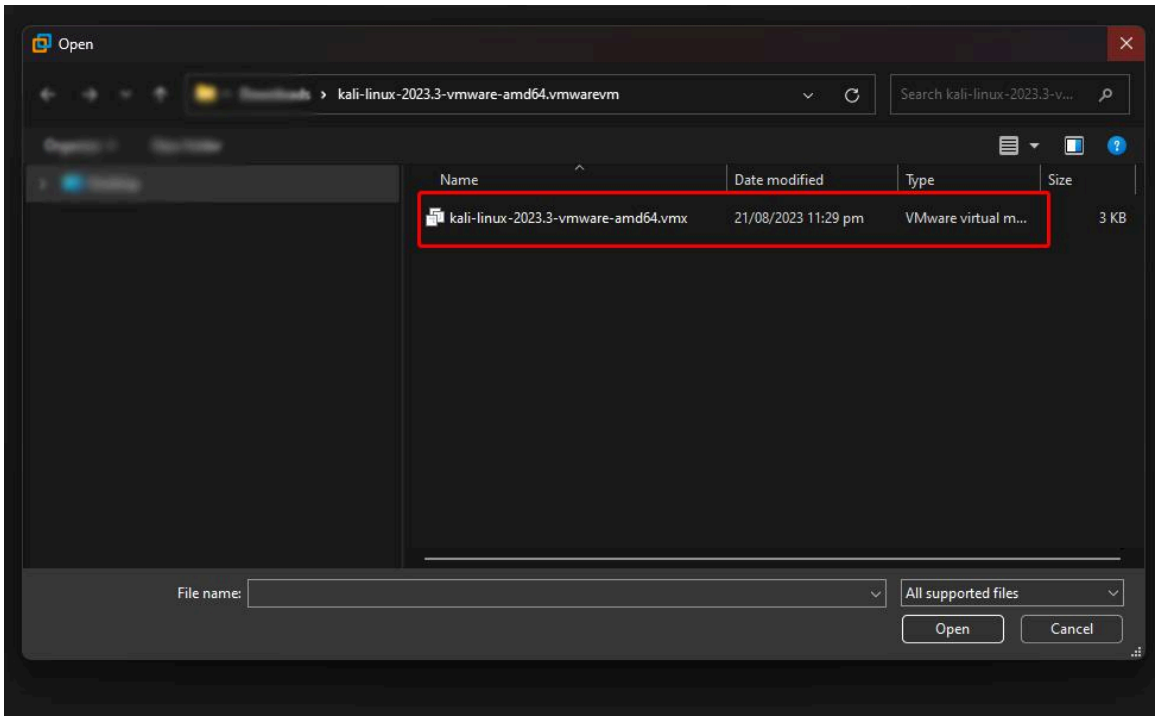
جـ/ الفرق بالنسخة المدفوعة تأتي بميزة الـ Snapshot Manager وهي ميزة للأنشاء نسخ احتياطية للأجهزة الافتراضية.

بعد تحميل وتنصيب البرنامج على الجهاز الخاص بك

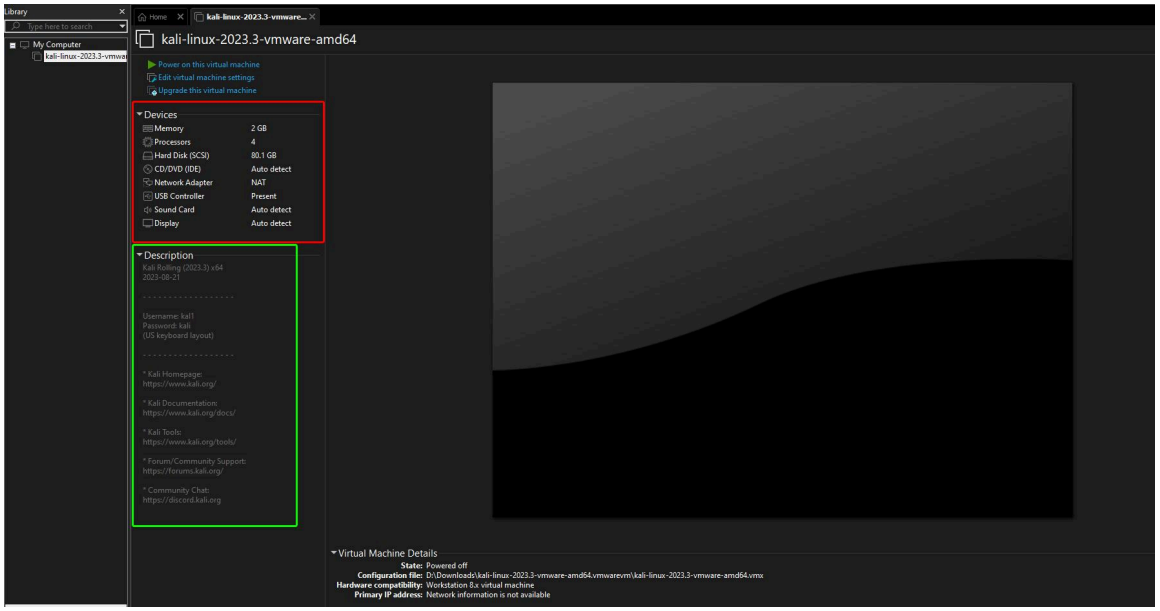
تنصيب Kali Linux اختيار Open a Virtual أو الاختصار على لوحة التحكم Ctrl + O



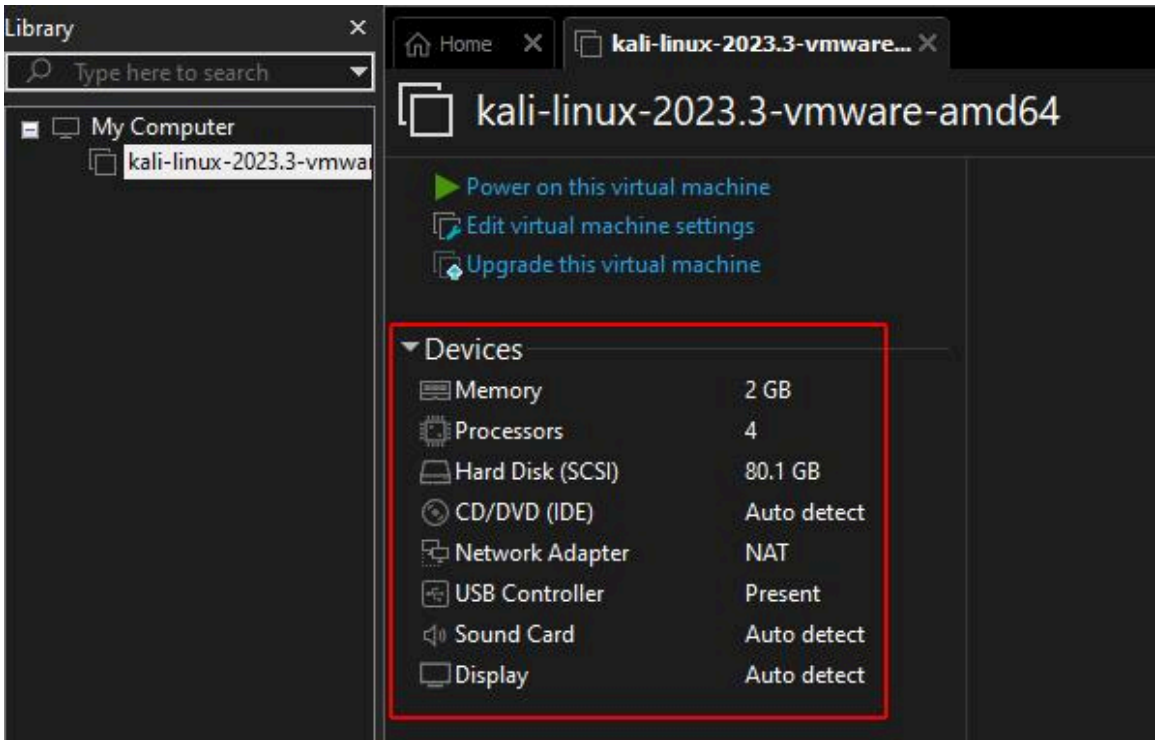
اختيار الملف المستخرج



بعد اختيار الملف ستظهر الصفحة التالية:



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



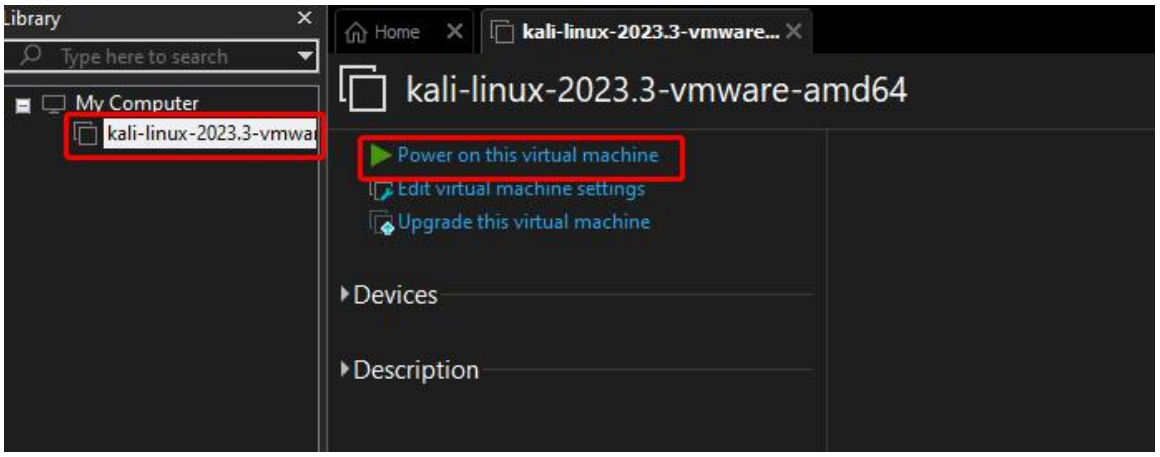
سـ/ ما هي المواصفات التي تشغل نظام Kali Linux ؟

جـ/ 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 كالـ Username و Password الخاصة بـ Kali وموقع الرسمي للنظام، ومواقع الأدوات الخاصة، وموقع دردشة المجتمع.

لتشغيل Kali Linux:

اختيار kali-linux ثم Power on this virtual

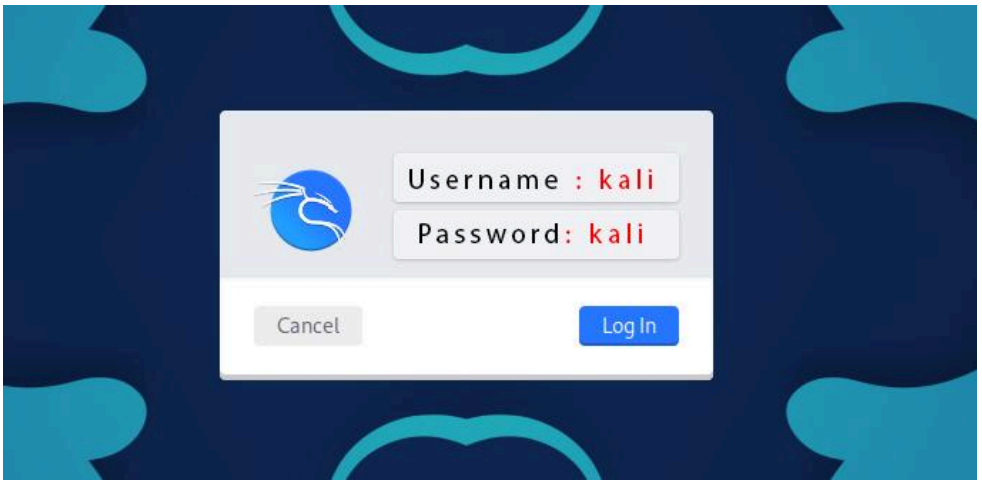


بعد التشغيل يجب اختيار Kali Linux بالضغط على زر Enter او الانتظار 5 ثواني للدخول تلقائياً

عند التشغيل سيطلب منك Username و Password للدخول

سـ/ ما هو Username والـ Password لنظام Kali وهل استطيع تغييرها ؟

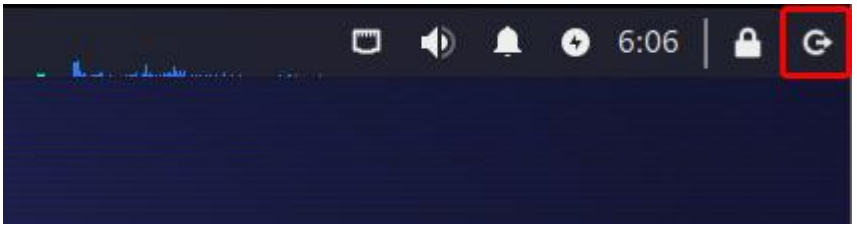
جـ/ نعم يمكن تغييرها



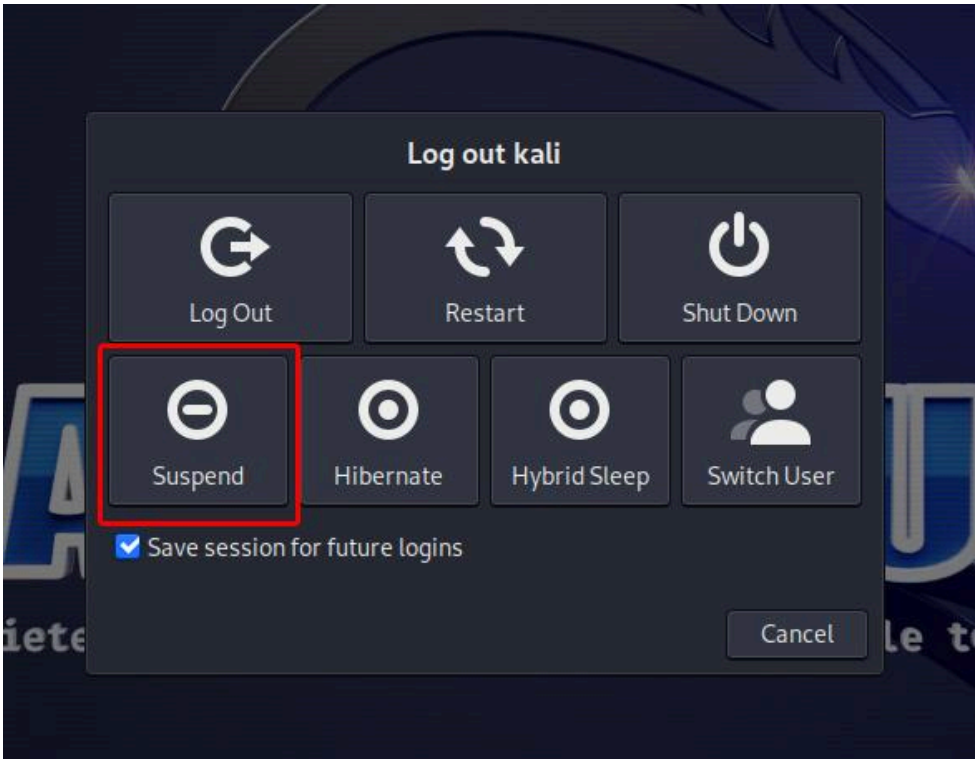
عند وصولك الى هذا المرحلة يمكنك البدء بإستخدام Kali Linux 🥳

تعريف الواجهة الرسومية لـ Kali Linux

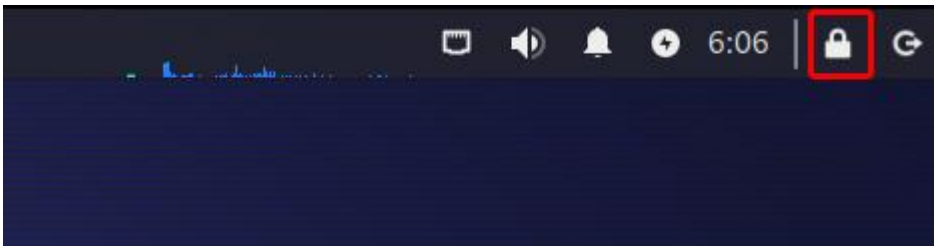
تدل الايقونة ادناه الى تسجيل الخروج من النظام



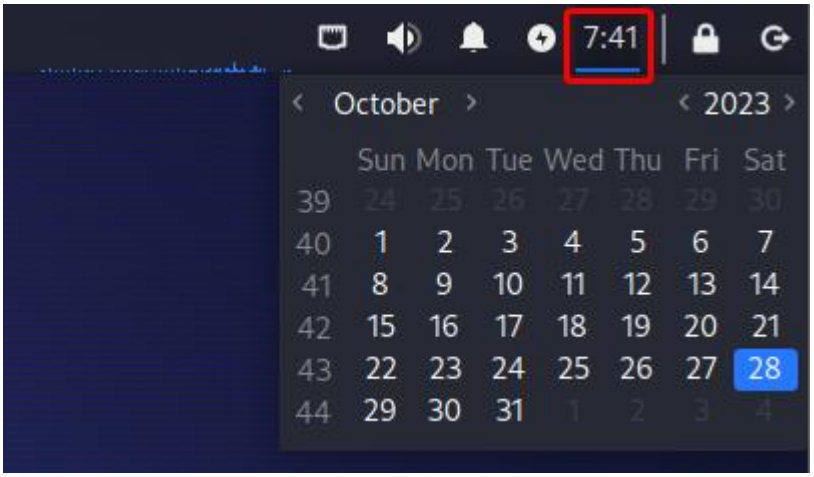
(يفضل عند تسجيل الخروج من النظام اختيار Suspend)



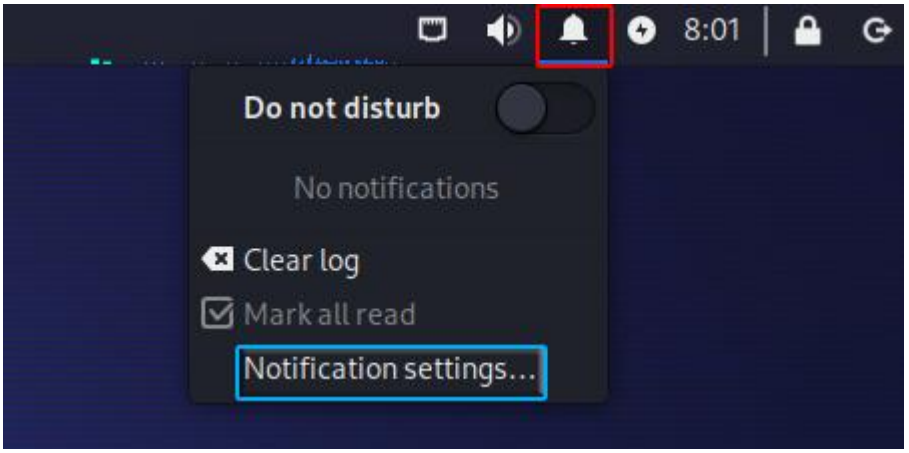
تدل الايقونة ادناه **Lock Screen** إلى إيقاف الشاشة



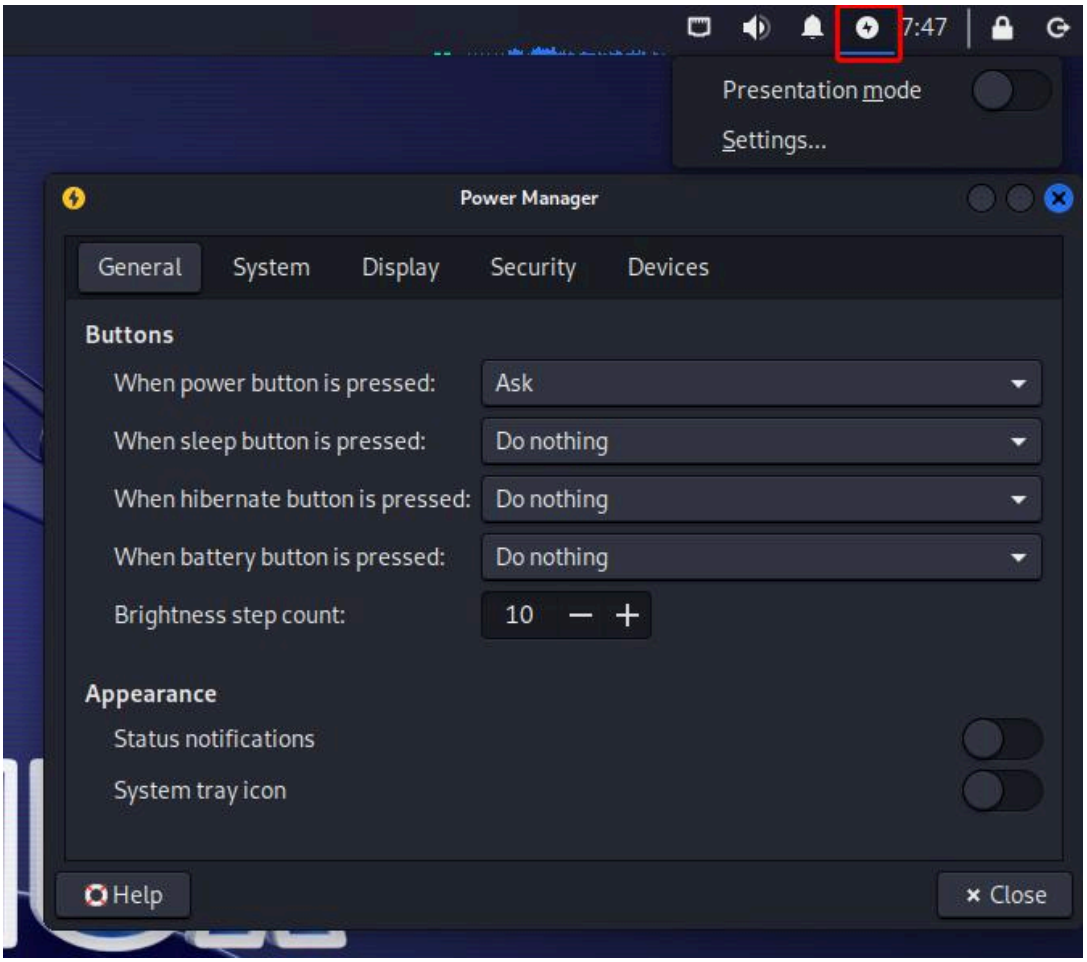
تدل الايقونة ادناه **The Date** إلى الوقت والتاريخ



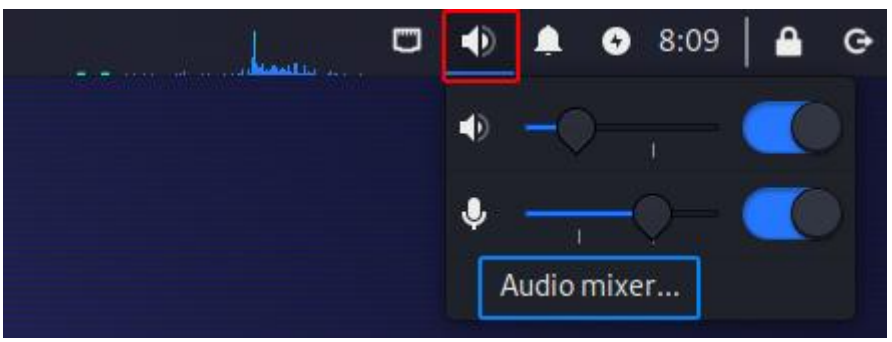
تدل الايقونة ادناه **Notifications** إلى الإشعارات في النظام، يمكن تغيير التحكم في الإشعارات من خلال **Notifications settings**



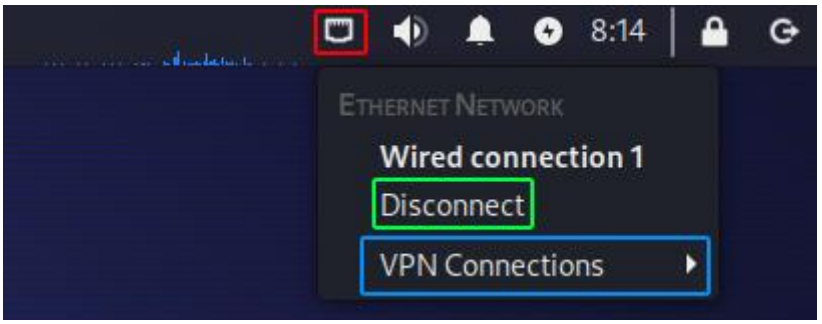
تدل الايقونة ادناه **Power Manager** إلى مدير الطاقة، والذي يمكنه أن يشمل العديد من الوظائف والإعدادات، ضبط إعدادات السطوع، إدارة وضع السكون، تخصيص إعدادات الطاقة.



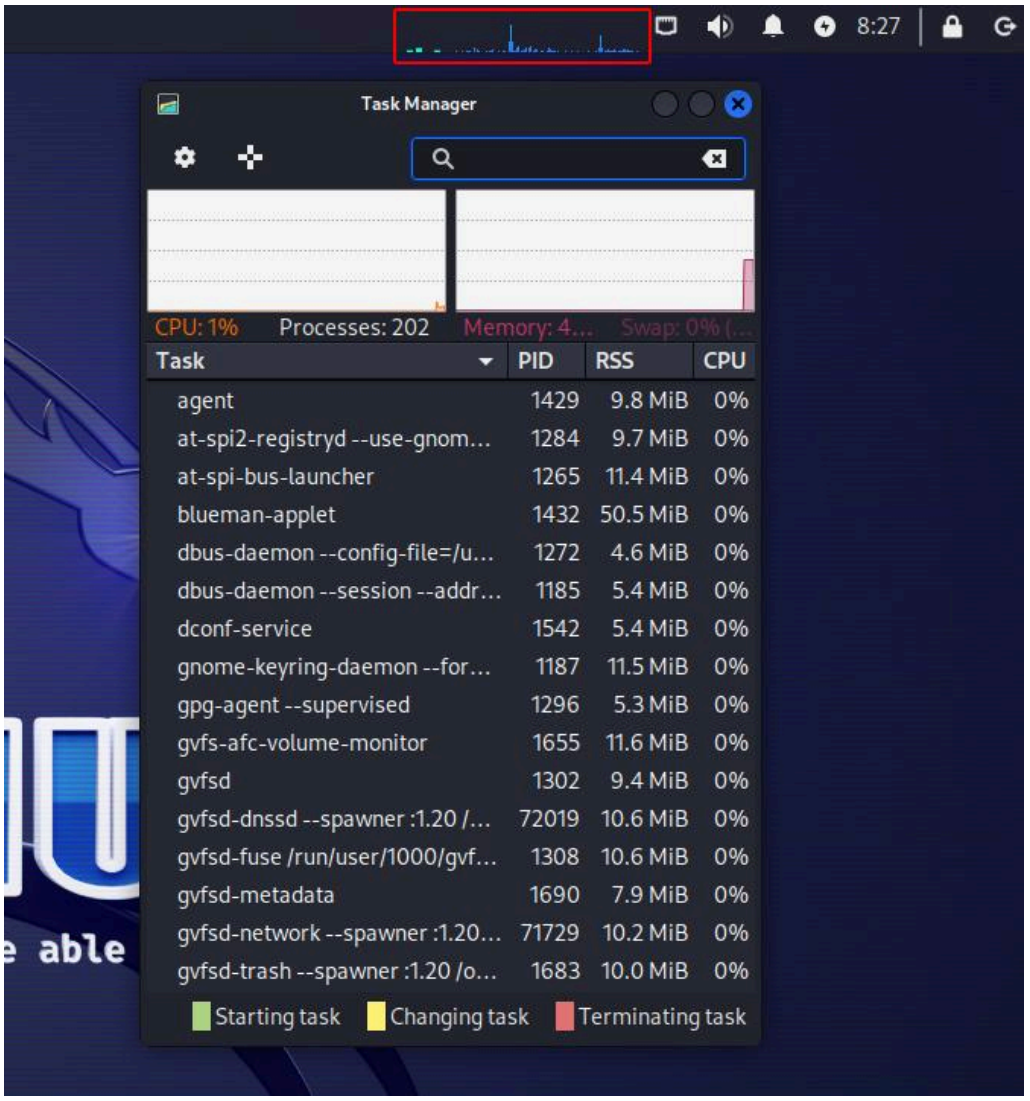
تدل الايقونة ادناه **The Sound** إلى نسبة الصوت والمايكروفون في النظام، يمكن ضبط إعدادات الصوت من خلال **Audio mixer**



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

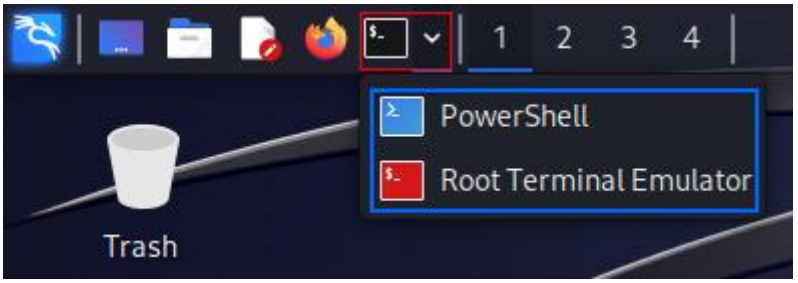


تدل الايقونة ادناه Task Manager إلى مراقبة وإدارة العمليات والمهام واستهلاك الموارد على النظام، تسمح بإنهاء العمليات، وهي مفيدة لأغراض الاختبار والتشخيص وإدارة المواد.

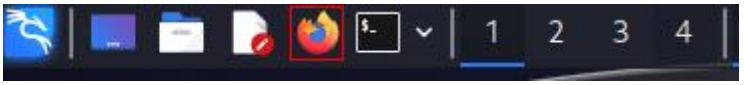


على الجهة اليسرى توجد أيقونات أخرى منها، أيقونة New desktop لإنشاء سطح مكتب آخر كما موضح ادناه.

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)



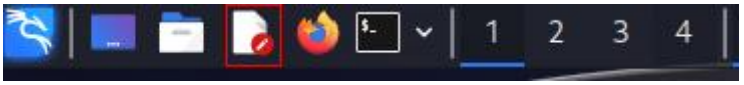
تدل الايقونة ادناه الى برنامج التصفح FireFox، لتصفح شبكة الإنترنت العالمية.



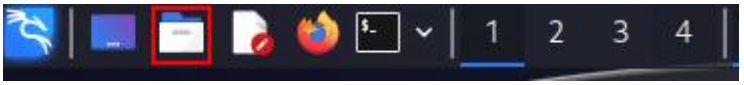
سـ/ هل يمكن تثبيت متصفحات اخرى غير FireFox ؟

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

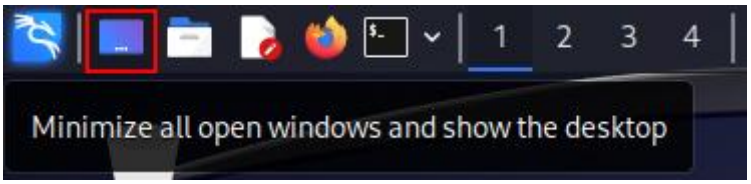
تدل الايقونة ادناه الى Text Editor، محرر نصوص للكتابة.



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.



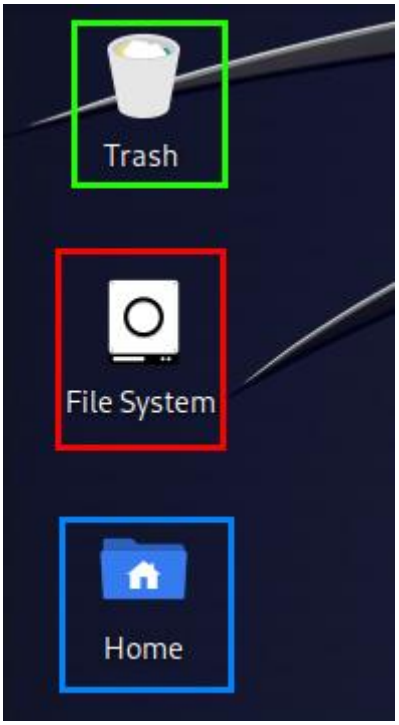
تدل الايقونة ادناه الى جميع الأدوات والبرامج المثبتة والغير مثبتة في نظام Kali.

تدل الايقونات الاخرى الى:

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

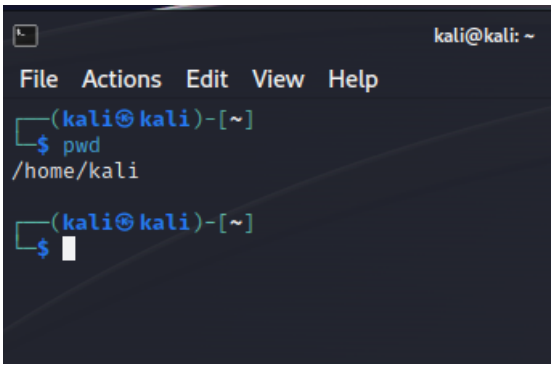
ملفات النظام: يحتوي على جميع ملفات النظام.

سطح المكتب: يحتوي على ملفات سطح المكتب الأساسية.

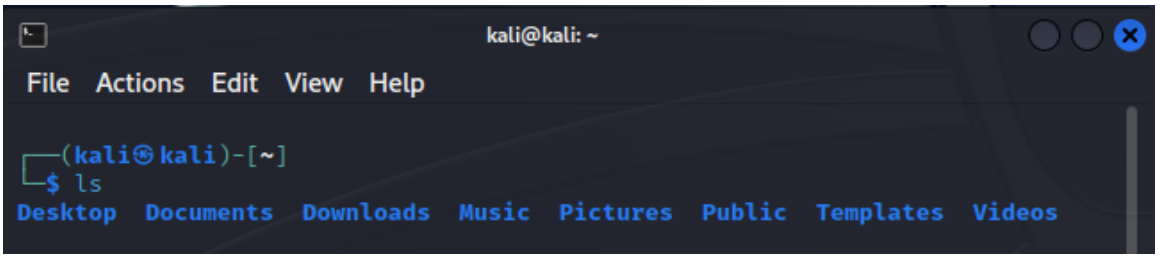


الأوامر الأساسية في نظام Kali Linux

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



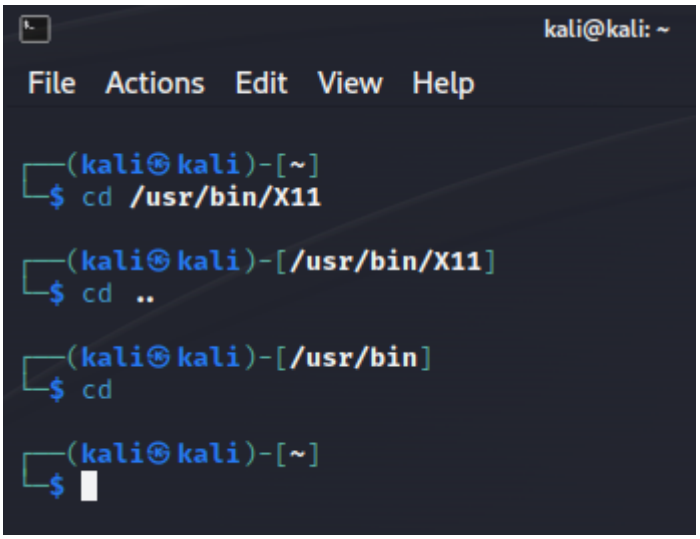
يستخدم لعرض محتوى المجلد الحالي :(List) ls



يستخدم للانتقال بين المجلدات :(Change Directory) cd

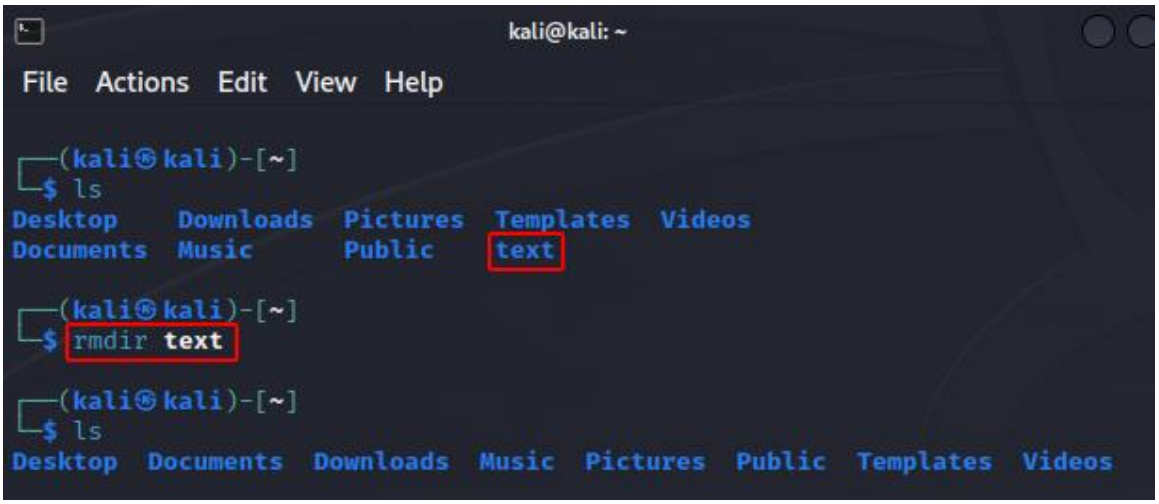
الرجوع خطوة الى الوراء cd ..

الرجوع الى الملف الرئيسي cd

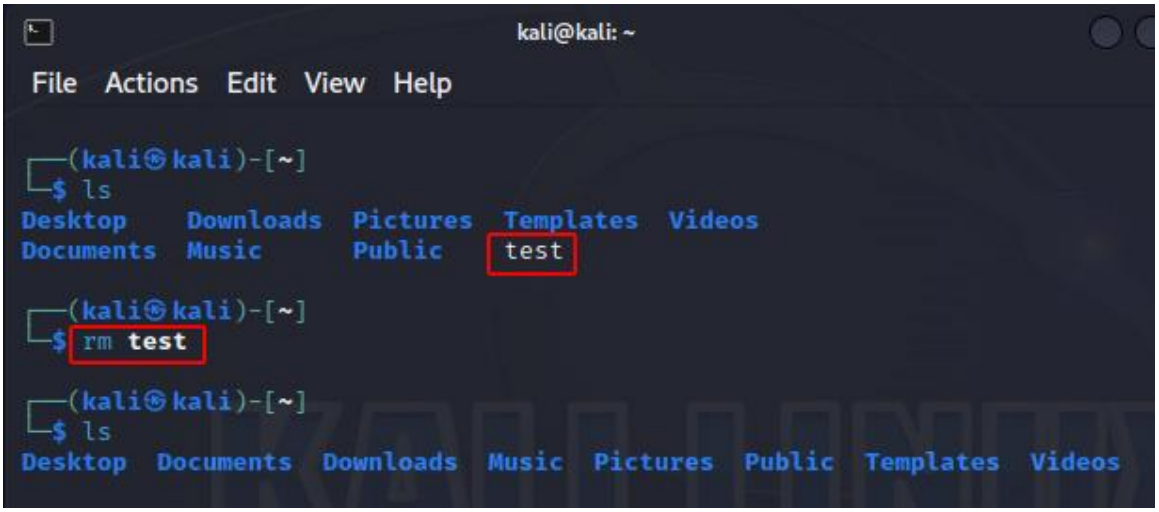


يستخدم لإنشاء مجلد جديد :(Make Directory) mkdir

يستخدم لحذف مجلد فارغ :(Remove Directory) rmdir



يستخدم لحذف ملف أو مجلد :(Remove) rm

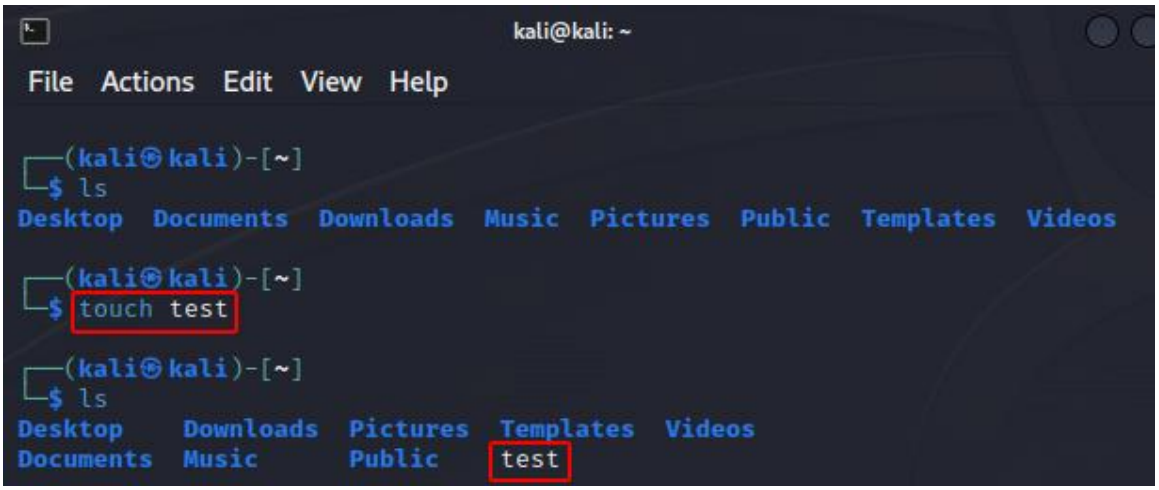


سـ/ ماهو الفرق بين أمر rmdi و rm ؟

جـ/ 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 فارغًا.

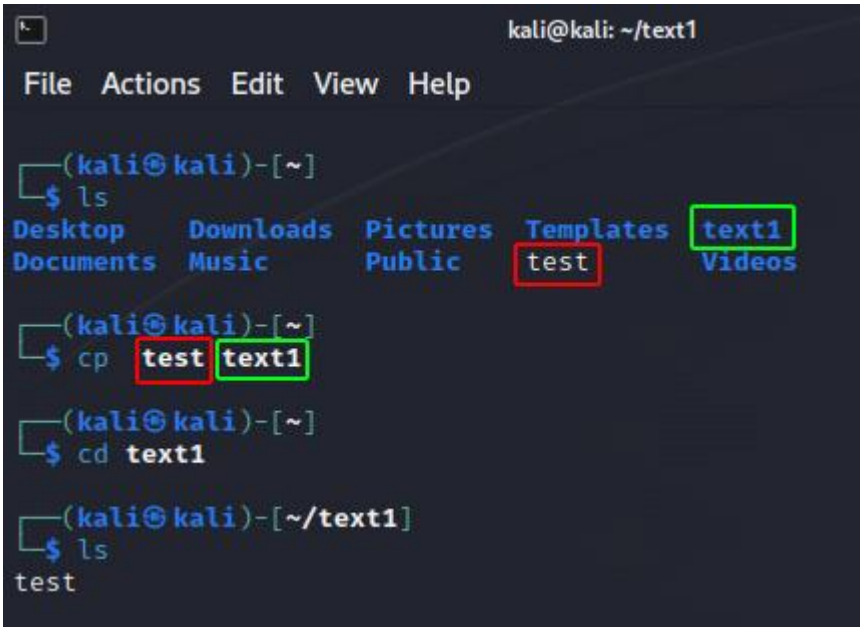
أمر rm مستخدم لحذف الملفات والمجلدات الفارغة وإيضاً لحذف المحتوى، بما في ذلك الملفات والمجلدات داخلها.

يستخدم لإنشاء ملف جديد :**touch**

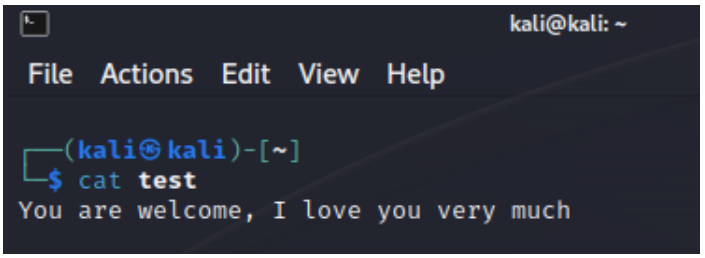


يستخدم لنسخ ملف أو مجلد :**cp** (Copy)

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

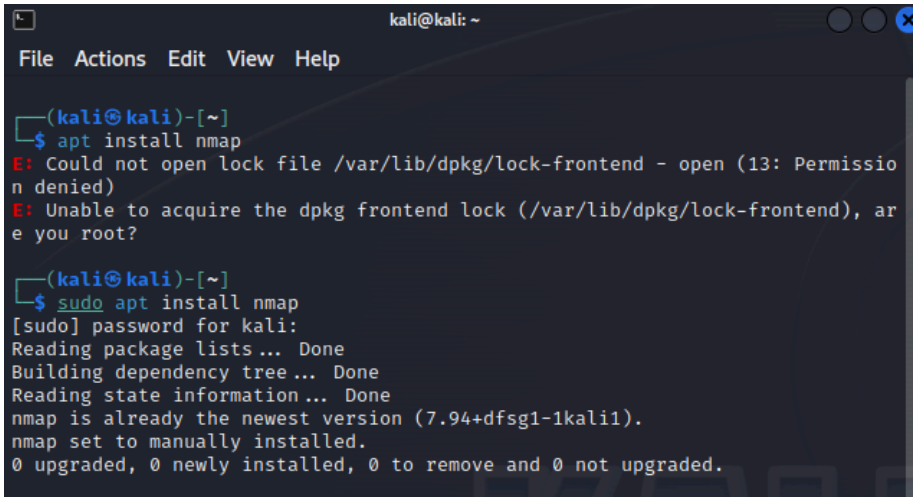


يستخدم لعرض محتوى ملف نصي :**cat**

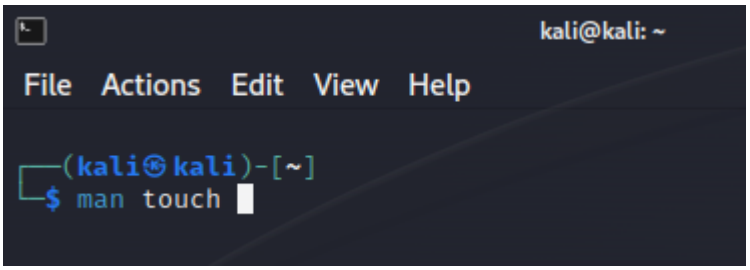


يستخدم لمسح الأوامر من الشاشة: **clear**

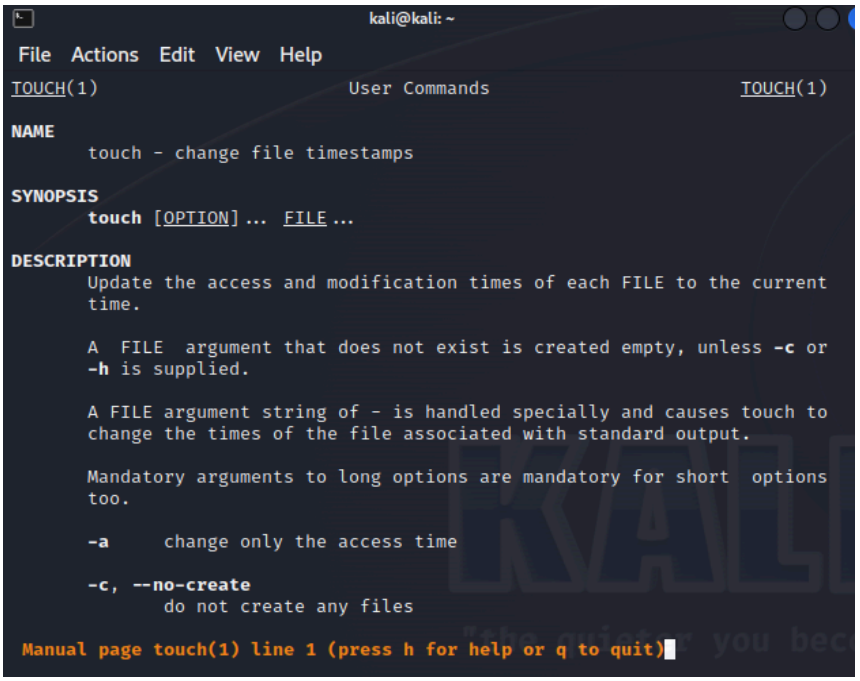
يستخدم لتنفيذ أمر بصلاحيات المسؤول root: **sudo**



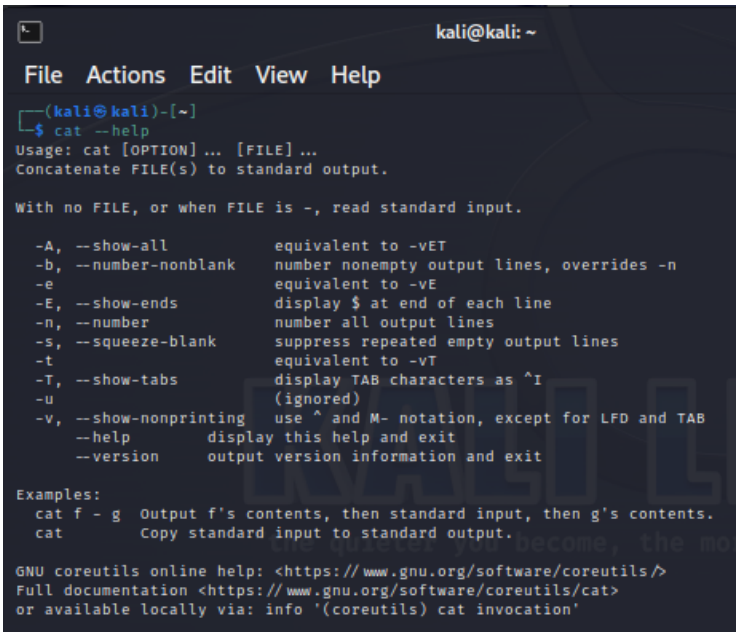
يستخدم للحصول على مساعدة مفصلة لأمر معين: **man**



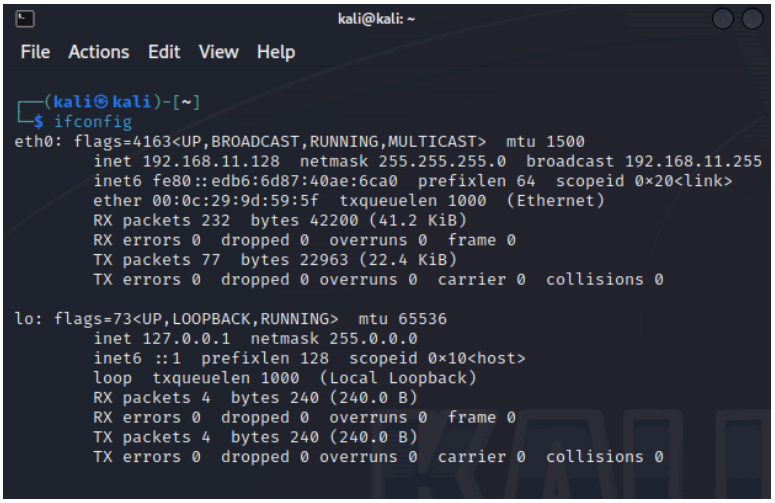
ستظهر صفحة كاملة لشرح الأمر بالتفصيل، للخروج اضغط حرف **Q**



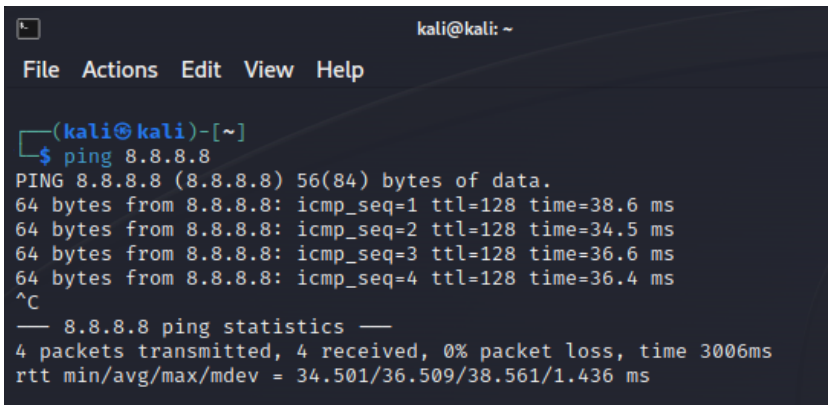
ايضا يمكن الحصول على المساعدة باستخدام أمر **--help** كما موضح ادناه



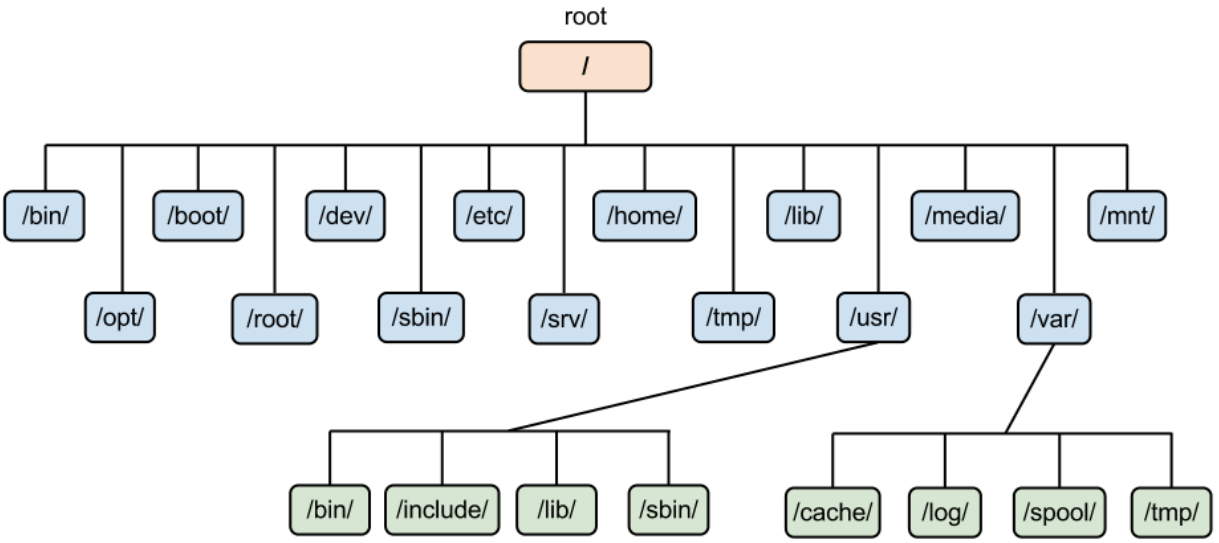
ifconfig: IPلعرض معلومات عن واجهات الشبكة وعناوين



ping: IP يستخدم لاختبار الاتصال بمضيف عبر شبكة



التسلسل الهرمي لنظام Kali Linux



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 mount ، cp ، ls 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 ديناميكيًا 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

(واجهة سطر الأوامر) Command Line interface CLI

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

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

(واجهة المستخدم الرسومية) Graphical User Interface GUI

يمكن تعيينه على وضع الوصول الافتراضي إذا تم تثبيته

يحتوي على قوائم وأيقونات ورسومات

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

أوامر مختلفة لإيقاف أو إعادة تشغيل النظام

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

إدارة حسابات المستخدمين والمجموعات

Root User / SuperUser	• 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	• 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

Normal User	• 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 كـ 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

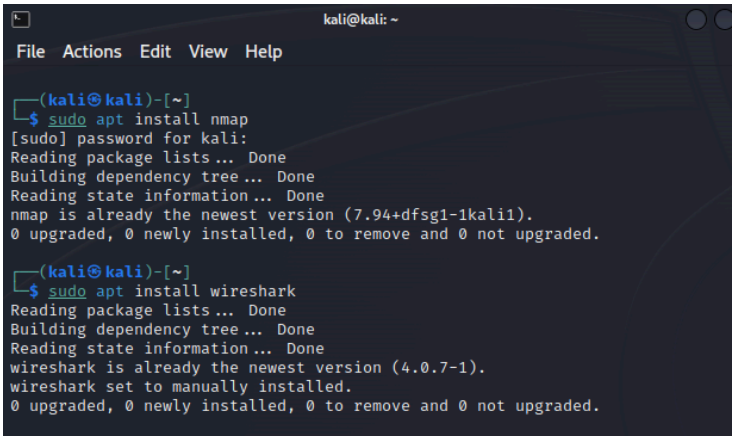
1- تحديث النظام باستخدام الأوامر:

sudo apt update

sudo apt upgrade

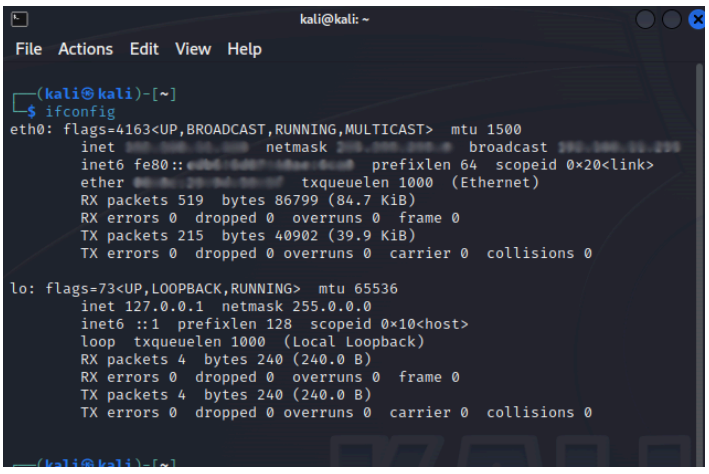
2- تثبيت أدوات الأمان يحتوي: Kali Linux على العديد من أدوات الأمان واختبار الاختراق

مُسبقة التثبيت. يمكنك استكشاف واستخدام هذه الأدوات لأغراض الاختبار والاستفادة منها، مثل Metasploit Framework , Wireshark , Nmap.



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:



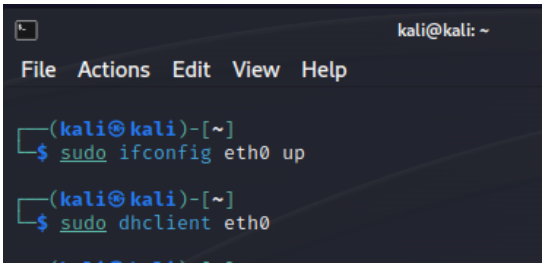
ابحث عن واجهة الشبكة التي ترغب في تكوينها، عادةً تكون مسماة بشكل مشابه لـ "eth0" للاتصال بالشبكة السلكية أو "wlan0" للاتصال بالشبكة اللاسلكية.

تكوين الشبكة السلكية (Ethernet):

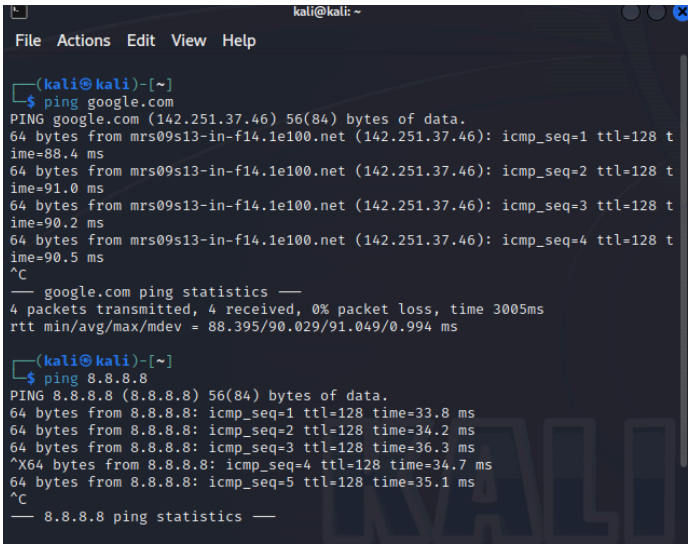
استخدام الأمر التالي لتفعيل الواجهة والحصول على عنوان IP بشكل تلقائي من خلال DHCP:

sudo ifconfig eth0 up

sudo dhclient eth0



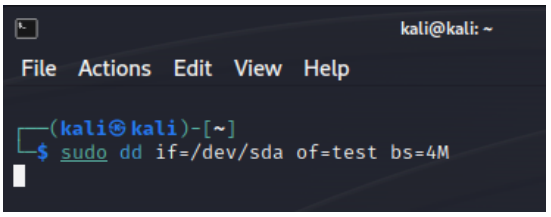
اختبار الاتصال: للتحقق من أنك متصل بالإنترنت بنجاح، يمكنك استخدام أمر "ping" مع عنوان IP أو اسم مضيف معروف. على سبيل المثال:



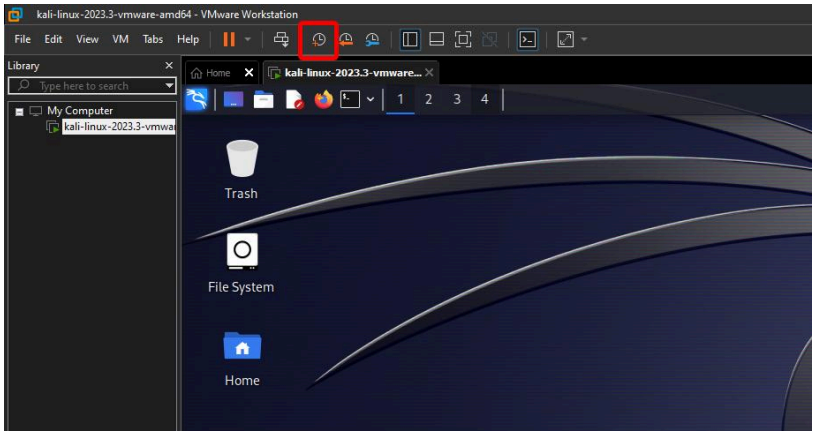
4- القيام بالنسخ الاحتياطي: قم بعمل نسخ احتياطية للبيانات الهامة والإعدادات قبل البدء في تكوين النظام، يمكنك استخدام "dd" لنسخ القرص الصلب بالكامل إلى ملف صورة أو قرص آخر. تأكد من توجيه النسخ الاحتياطي إلى وجهة آمنة.

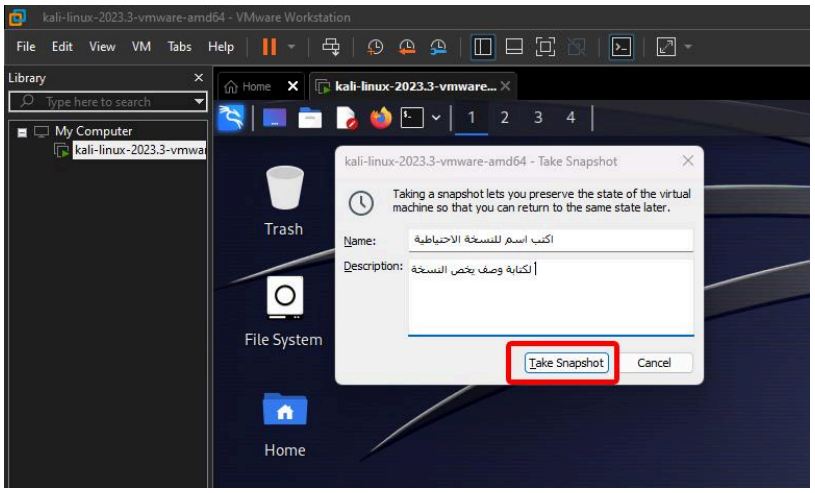
لاستخدام "dd" لنسخ القرص:

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

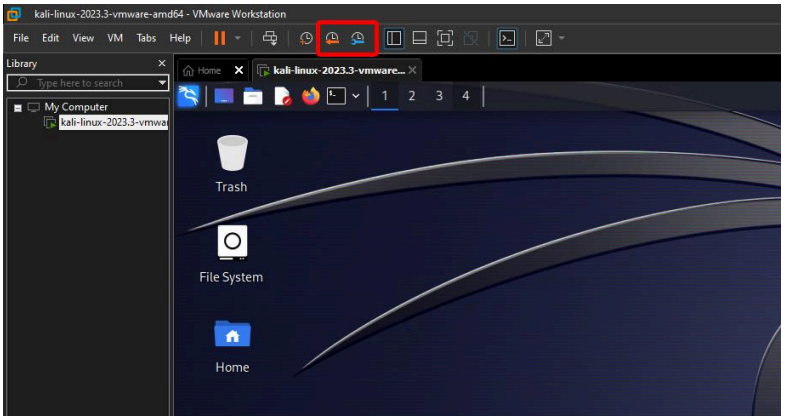


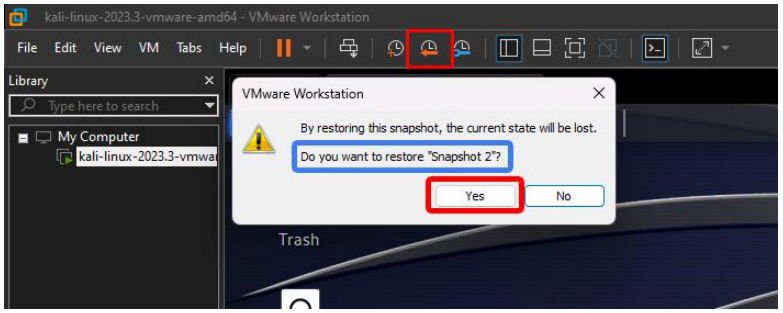
ايضاً يمكنك عمل نسخ احتياطية للنظام من برنامج Workstation Pro باستخدام ميزة snapshot:



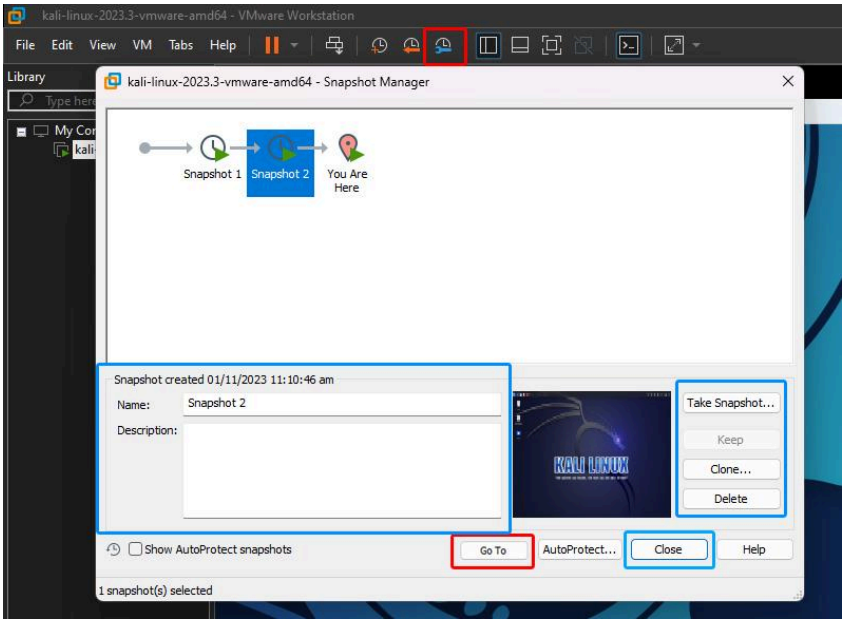


للرجوع الى النسخة الاحتياطية السابقة:





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



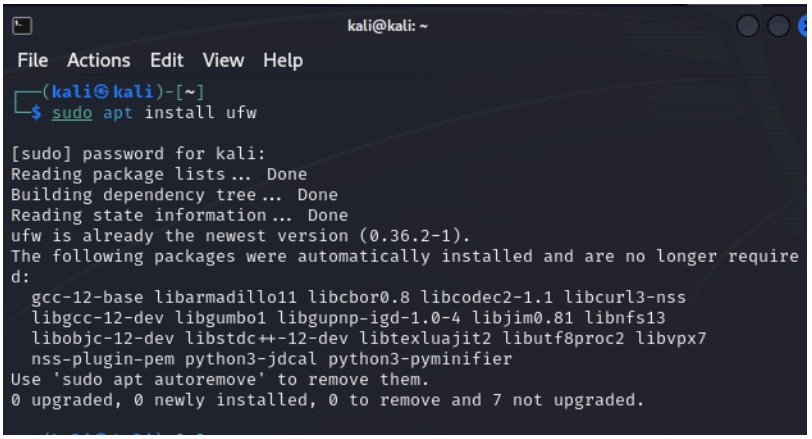
5- تعلم وتحسين مهارات الاستخدام: Kali Linux تتيح لك الوصول إلى مجموعة واسعة من أدوات الأمان واختبار الاختراق. قم بتعلم كيفية استخدامها بشكل فعال وتحسين مهاراتك.

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.

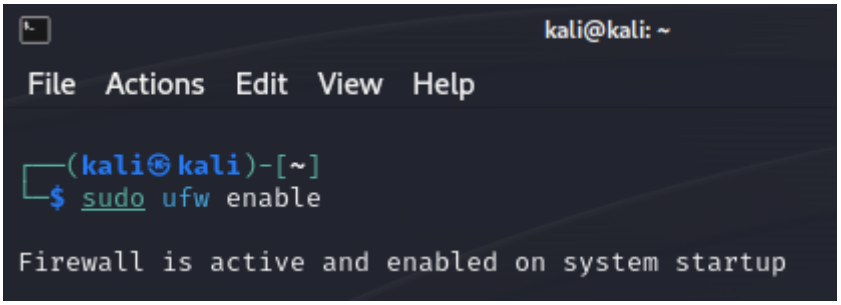
تكوين جدار حماية قم بتثبيت الأمر UFW:

sudo apt install ufw



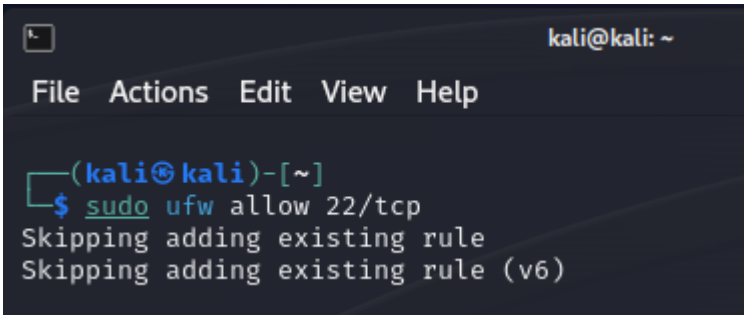
بعد التثبيت، قم بتفعيل UFW باستخدام الأمر:

sudo ufw enable



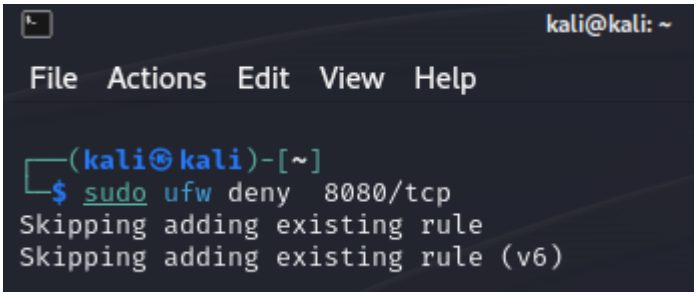
يمكنك تكوين قواعد الجدار وتحديد الخدمات والمنافذ التي ترغب في السماح بالوصول إليها ومنع الوصول إليها. على سبيل المثال، للسماح بالوصول إلى SSH (المنفذ 22):

sudo ufw allow 22/tcp



لمنع الوصول إلى منفذ معين (منفذ 8080 كمثال):

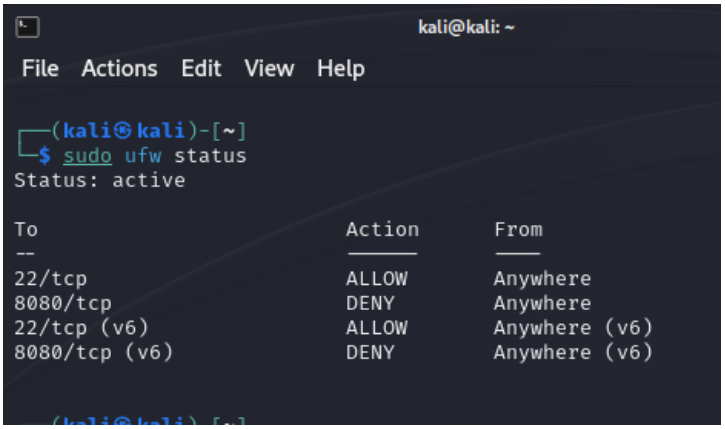
sudo ufw deny 8080/tcp



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

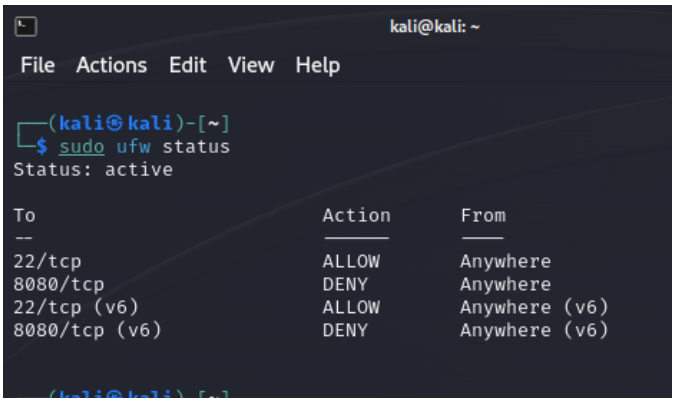
يمكنك التحقق من حالة UFW باستخدام أمر:

sudo ufw status



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

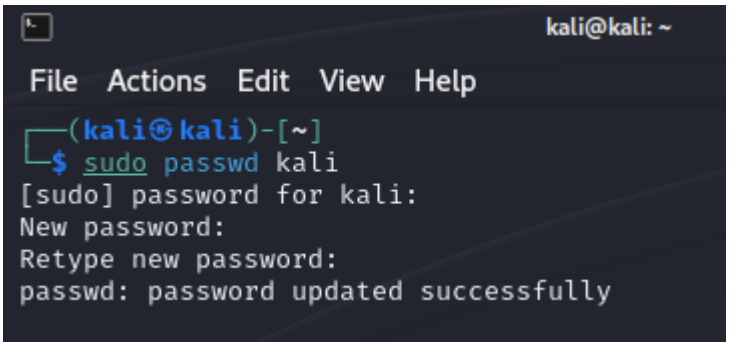
sudo systemctl enable ufw



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

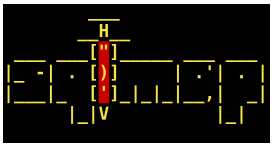
استخدم الأمر "passwd" مع اسم المستخدم لتغيير كلمة المرور. أدخل الأمر التالي واستبدل "username" بالاسم الذي ترغب في تغيير كلمة مروره:

sudo passwd username



أهم أدوات Kali Linux

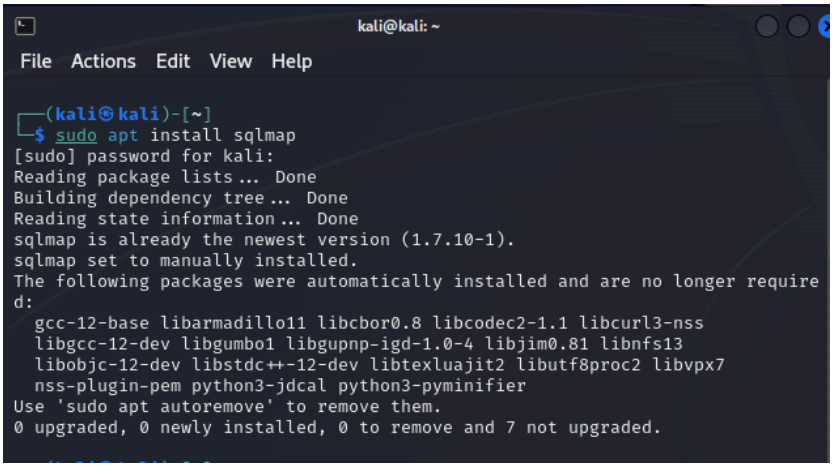
اسم الأداة	الوظيفة	الشعار
Nmap	أداة مسح الشبكة التي تستخدم لفحص الشبكات واكتشاف الأجهزة والخدمات المتاحة عليها	
Wireshark	برنامج مراقبة حركة البيانات عبر الشبكة، يمكن استخدامه لتحليل حركة الشبكة واكتشاف الهجمات	
Metasploit Framework	منصة قوية لاستغلال الثغرات واختبار الأمان، تمكن محترفي الأمان من اختبار 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

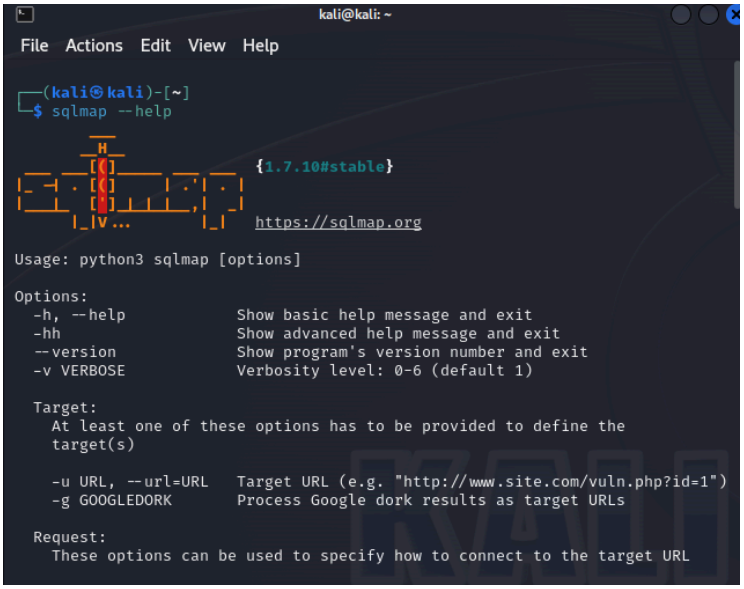
مثال:



إذا كنت تريد المساعدة حول أي أداة من الأدوات أعلاه استخدم أمر :

--help

مثال:



إدارة حسابات المستخدمين والمجموعات

المستخدم

إنشاء مستخدم جديد	useradd
لتعديل صلاحيات المستخدم او اضافته لمجموعة	usermod -G
حذف المستخدم	userdel
إعادة تعيين كلمة المرور	passwd

للمزيد من التفاصيل حول أمر معين استخدم help --

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

المجموعات

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

للمزيد من التفاصيل حول أمر معين استخدم help --

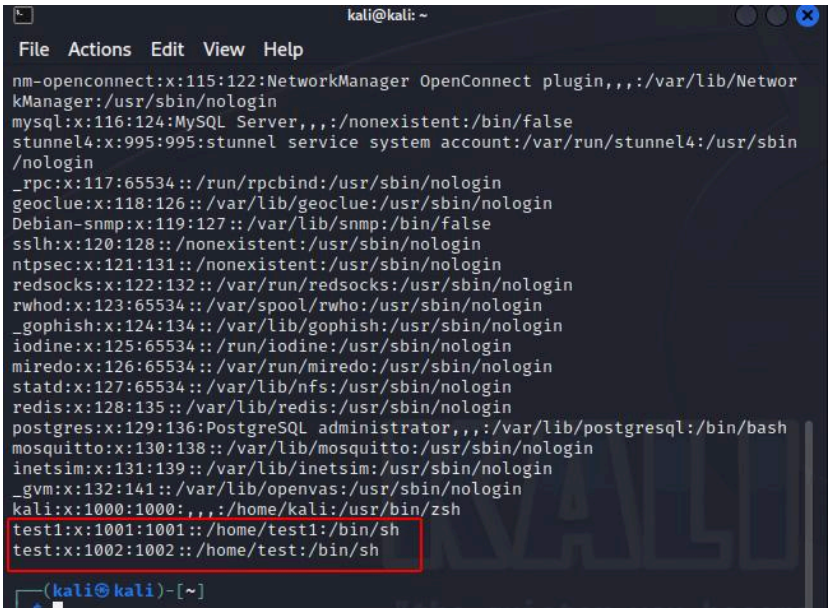
groupadd--help
groupmod--help
gpasswd--help
gropdel--help

المعلومات المخزنة حول المستخدمين و المجموعات

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

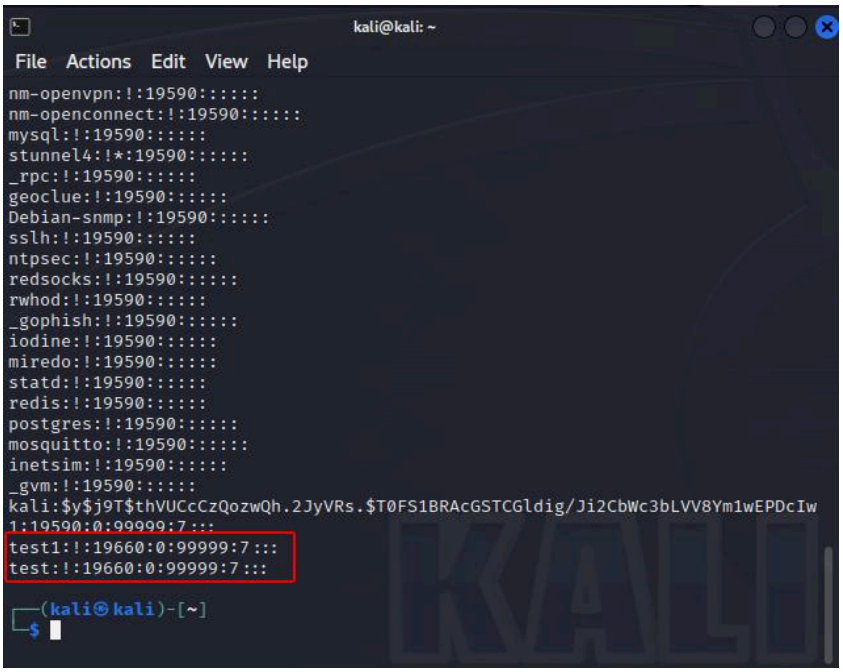
لمعرفة المستخدمين من خلال:

sudo cat /etc/passwd



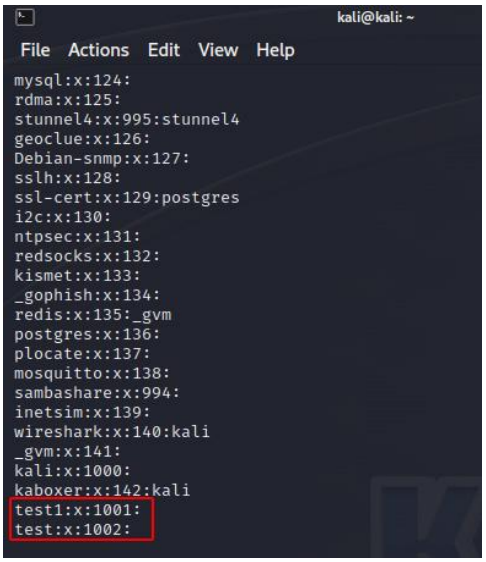
اسم المستخدم	معرف المستخدم	كلمة المرور	معرف المجموعة	وصف المستخدم	ملف المستخدم	نوع Shell
test	1002	xxxxx	1002	مستخدم عادي	/home/user1	/bin/bash

sudo cat /etc/shadow



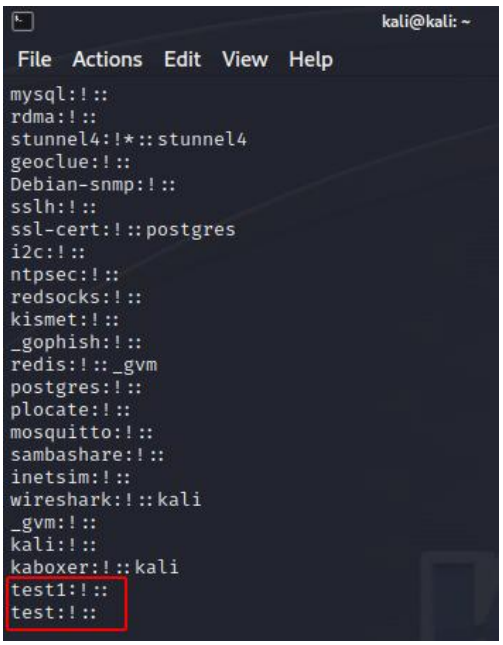
لمعرفة المجموعات من خلال:

sudo cat /etc/group



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

sudo cat /etc/gshadow



أنواع الملفات المختلفة في لينكس

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

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

تعديل الأذونات

الطريقة العددية	الطريقة الرمزية
• Read = 4 • Write = 2 • Execute = 1 • Total permission = 7 يستخدم أمر chmod 664 file 1 لتعديل إذن الملف.	• user (u) • group (g) • others (o) • all (a) • mean add (+) • means remove (-) • means Set (=) يستخدم أمر chmod لتعديل الأذونات على الملفات أو المجلدات. يمكن تعديل إذن واحد أو أكثر في نفس الوقت.

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 لتفعيل ملفات التبادل أو أقسام التبادل
33	swapon -a	يستخدم لتفعيل 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 تمكنك التصفح والتمرير خلفيًا 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 يهمه هذا الموضوع بهذا المقال.

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