À propos de Kali Linux

Kali Linux (anciennement connu sous le nom de BackTrack Linux) est une distribution Linux open source basée sur *Debian* destinée aux tests de pénétration avancés et à l'audit de sécurité.

Kali Linux contient plusieurs centaines d'outils destinés à diverses tâches de sécurité de l'information, telles que les tests d'intrusion, la recherche en sécurité, l'informatique judiciaire et l'ingénierie inverse aussi très bien réputé pour l'ethical hacking.

Kali Linux est une solution multiplateforme, accessible et disponible gratuitement pour les professionnels de la sécurité de l'information et les amateurs.

Kali Linux est sorti le 13 mars 2013 en tant que reconstruction complète et de haut en bas de *BackTrack Linux*, adhérent complètement aux normes de développement Debian.

Kali Linux vous convient-il ?

En tant que développeur de la distribution, vous pouvez vous attendre à ce que nous recommandions à tout le monde d'utiliser Kali Linux. Le fait est, cependant, que Kali est une distribution Linux spécifiquement destinée aux testeurs d'intrusion professionnels et aux spécialistes de la sécurité, et compte tenu de sa nature unique, ce n'est PAS une distribution recommandée si vous n'êtes pas familier avec Linux ou si vous recherchez une distribution de bureau Linux à usage général pour le développement, la conception Web, les jeux, etc.

Même pour les utilisateurs expérimentés de Linux, Kali peut poser des problèmes. Bien que Kali soit un projet open source, ce n'est pas un projet open source à grande échelle, pour des raisons de sécurité. L'équipe de développement est petite et fiable, les packages dans les référentiels sont signés à la fois par le commuter individuel et l'équipe, et - ce qui est important - l'ensemble de référentiels en amont à partir desquels les mises à jour et les nouveaux packages sont extraits est très petit.

Dans ce tutoriel nous allons voir comment installer la distribution Kali Linux dans un contexte éthique pour se former à la cybersécurité.

📌Site officiel Kali Linux: https://www.kali.org/
📌Download Kali Linux: https://www.kali.org/get-kali/

SOMMAIRE

Dans les pages suivantes, la procédure étape par étape pour configurer les fonctions décrites ci-dessus sera expliquée avec une explication d'accompagnement :

Dans ce tutoriel, nous utiliserons Kali en dual boot et en WDS

Il sera possible de récupérer toutes **les images** en haute résolution en cliquant ici ou s'il s'agit d'une version imprimée, au lien suivant :
https://drive.google.com/drive/folders/13fLYMwxyZX-XxRDolzfb36X1bCZSmmX0?usp=sharing

Raccourci	Explication
GUI	Graphics user interface – Interface graphique
nmap	Network mapper
dual boot	installation de deux systèmes d'exploitation sur un seul ordinateur
WDS	Windows Deployment Services

Remarque:
Cette leçon/tutoriel est uniquement à des fins éducatives et tous les tests ont été effectués dans un environnement contrôlé. Toute tentative de reproduction dans des contextes de nature différente et/ou à des fins malveillantes constitue un crime informatique.

Kali est utilisé depuis la deuxième saison de la populaire série MR Robot. Bien que les hacks de la série puissent sembler fantastiques, Kor Adana, écrivain et producteur de technologie pour "***Mr. Robot***", dit qu'ils sont tout à fait plausibles. Adana a une formation en cybersécurité et il travaille avec une équipe de hackers expérimentés pour développer les scénarios technologiques de "Mr. Robot". Après que des millions de personnes l'ont regardé, des communautés ont commencé à se former.

1. Installation de Kali Linux

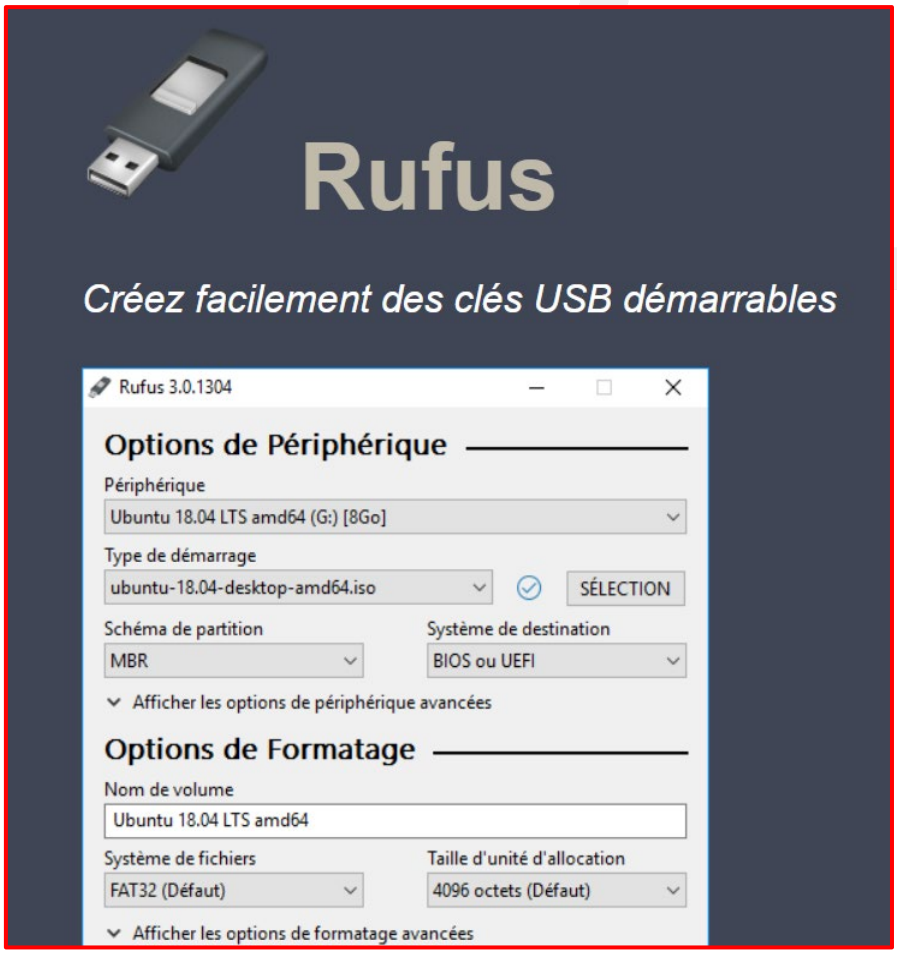
Pour installer Kali Linux diverses possibilités s'offrent à nous. Nous avons la possibilité de passer soit via un hyperviseur (type 1 ou type 2 Hyper V, VmWare etc…) ou via la nouvelle plateforme WSL (Windows subsystem for Linux).

Cette dernière option nous permet d'exécuter un environnement Linux sur un système Windows.
Nous avons décidé pour ce tutoriel de montrer l'installation en dual-boot ainsi que l'installation de KALI via WSL.

1.1. Dual Boot Kali Linux (Windows 10 - Kali)

Création d'une ''Live USB'' avec l'utilitaire Rufus

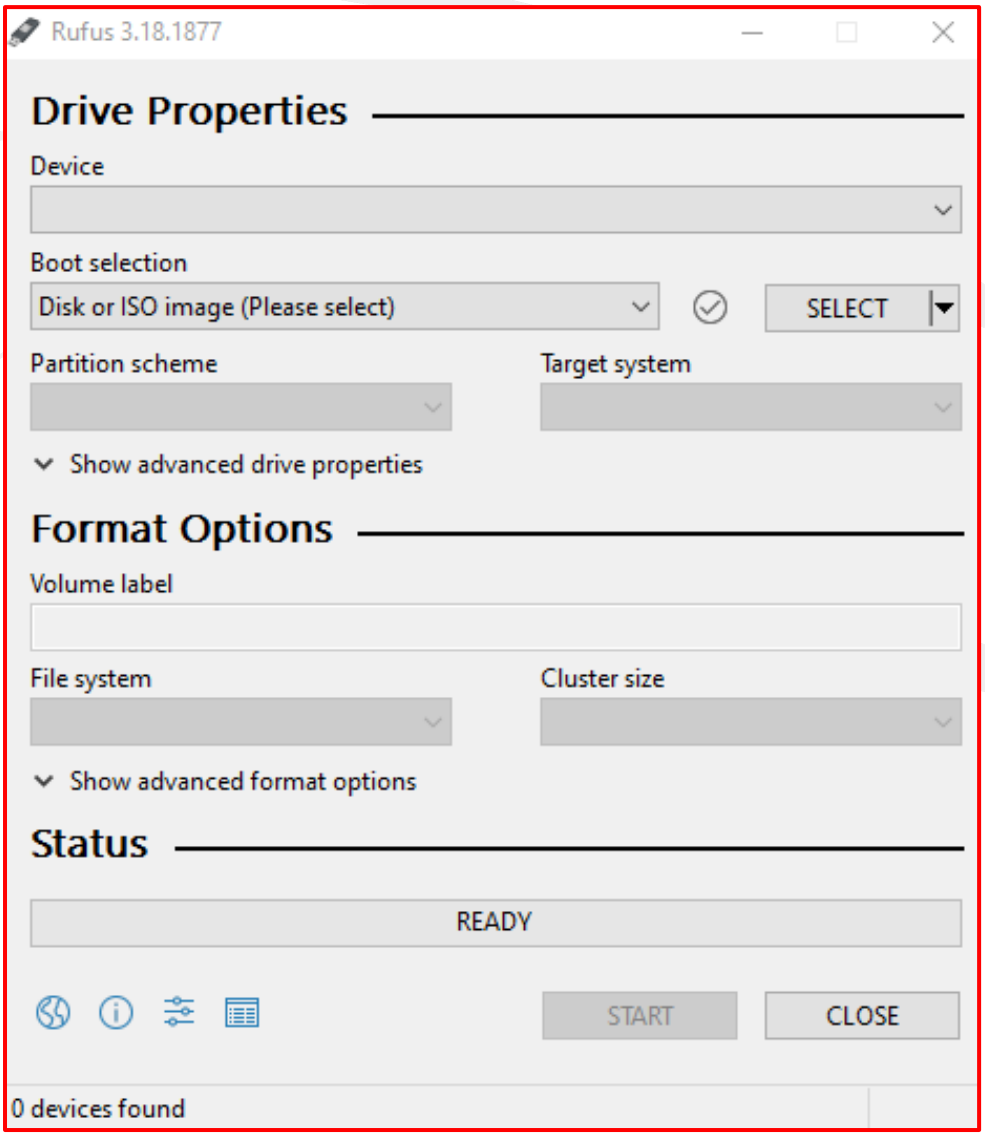
- Pour télécharger ***Rufus*** taper dans la barre de recherche Google "Rufus téléchargement" et téléchargez la Version .exe en bas de la page du site.



Une fois Rufus téléchargé exécutez-le et ouvrez le programme

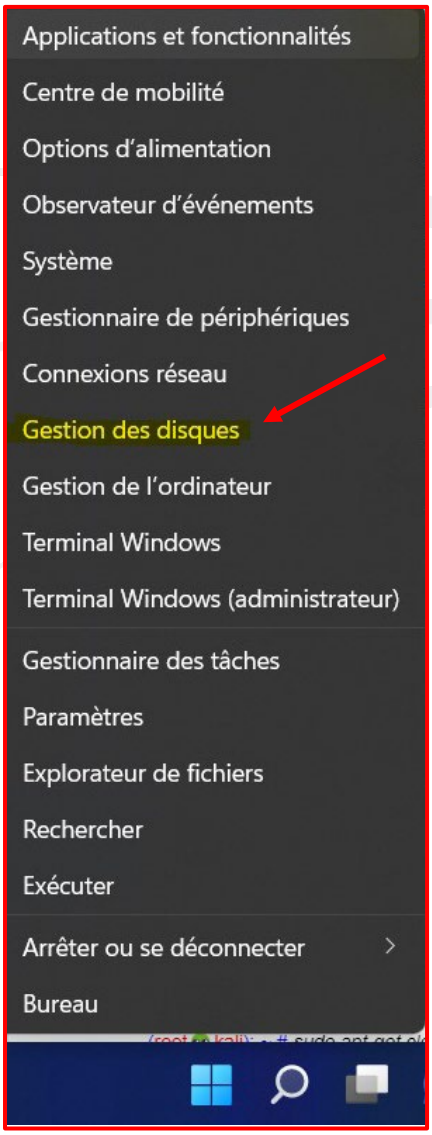
- Assurez-vous en parallèle d'avoir téléchargé l'Iso de Kali via le site que nous recommandons www.kali.org/get-kali/ .

- Via l'interface du programme Rufus : Choisissez le support (USB, disque externe etc..) que vous allez rendre bootable. > Et sélectionnez ensuite l'ISO dans le répertoire ou vous l'avez placé. Vous pouvez laissez le réglage en FAT32

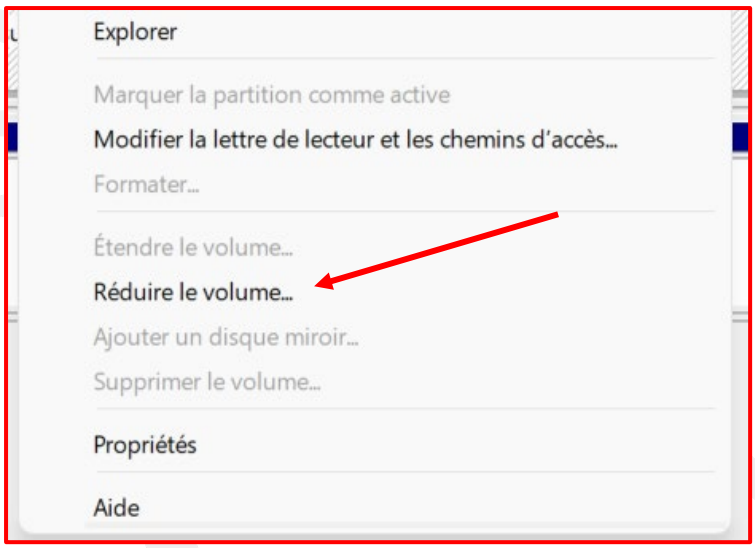


Créer une partition dédié à Kali Linux dans la gestion des disques

Faites un clic-droit sur Windows sur votre menu démarrer ou logo Windows

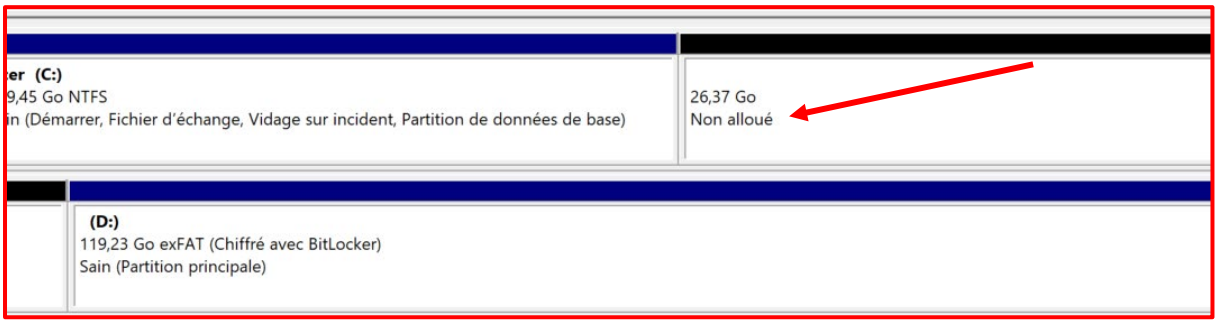


- Après avoir cliqué sur la Gestion des disques > Sélectionnez le volume système que vous souhaitez réduire…

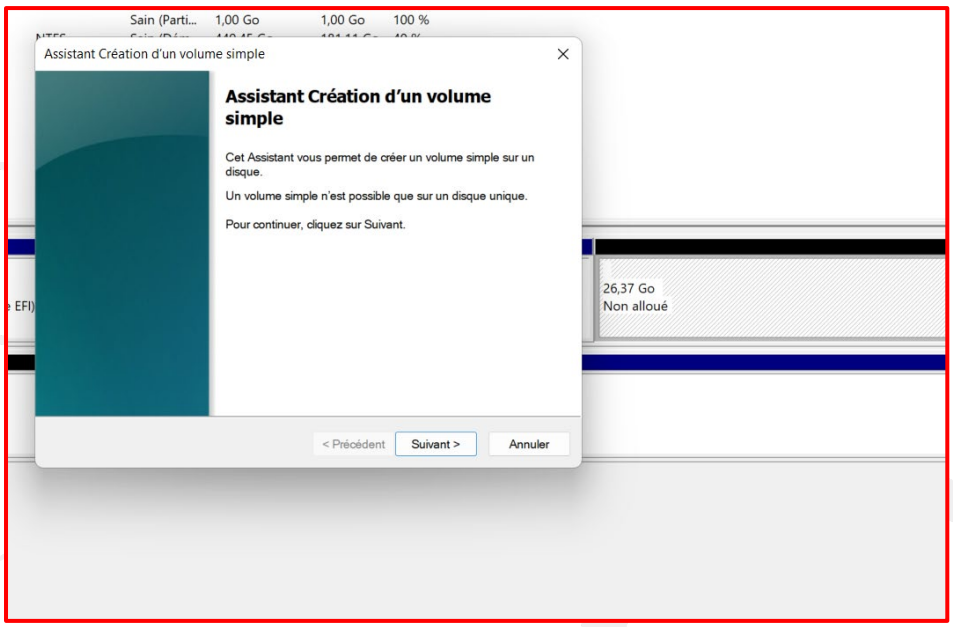


- Nous vous recommandons à minima de réduire et d'allouer 25 Go pour Kali Linux choisissez alors : 25 000 Mb

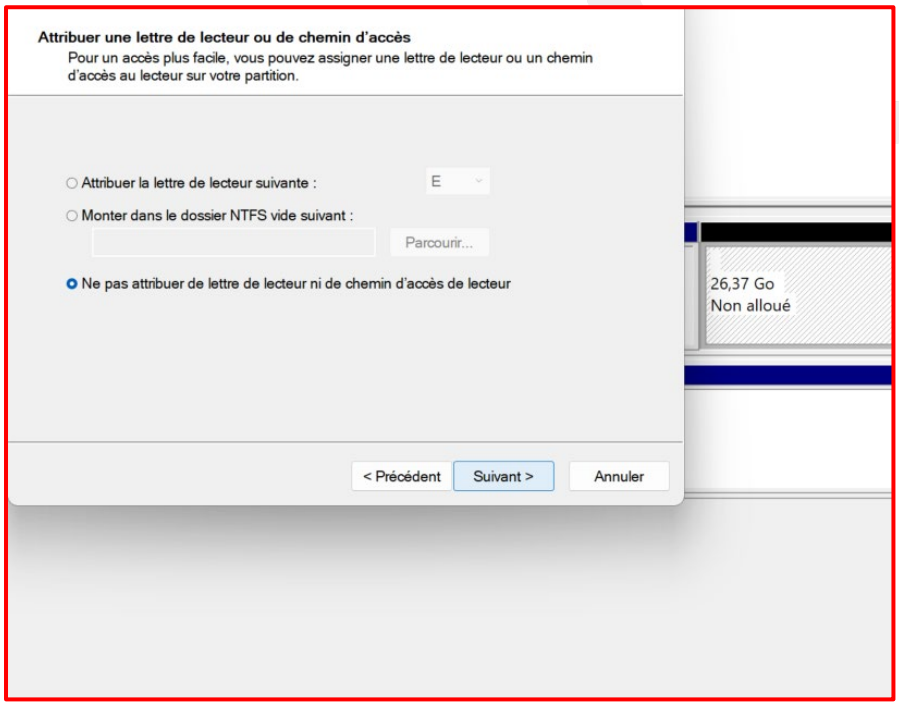
‘



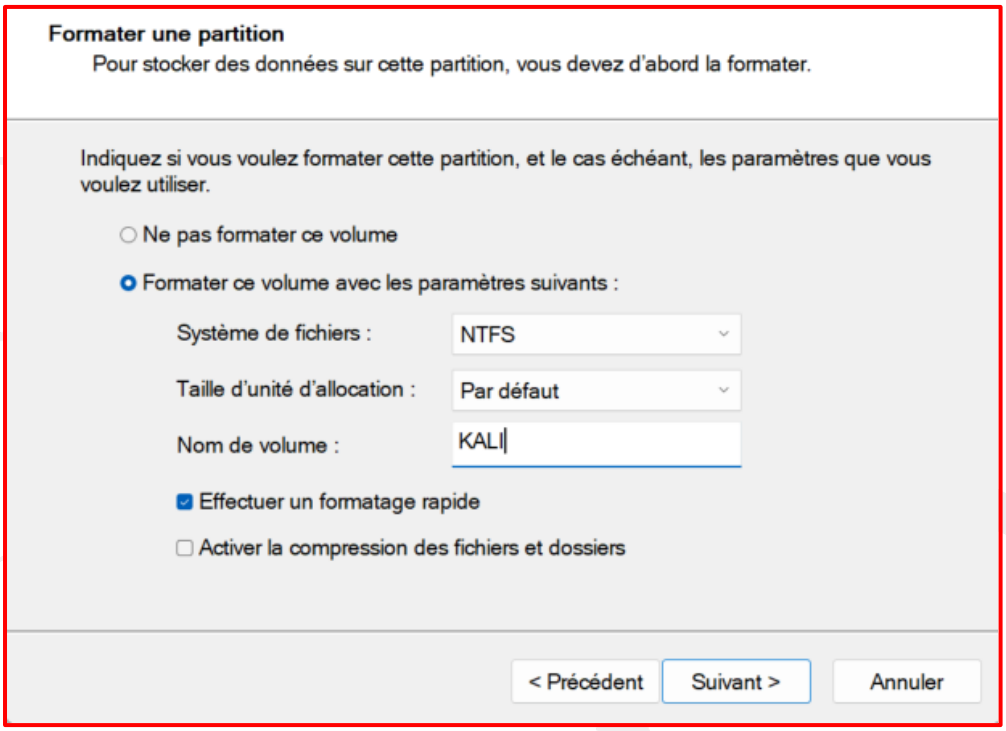
- L’objectif de créer une partition dans notre gestionnaire de disque est d'exécuter notre système d’exploitation Kali tout en gardant notre système d’exploitation principale Windows 10.



- Créer un volume de 25 Gb en NTFS .



- Donnez le nom que vous souhaitez au volume ici nous l'appelons << Kali>>
-
- Validez le formatage sur suivant



Préparation du support d'installation Clé USB etc…

- Maintenant que votre support est prêt à être inséré et que votre partition est préparée.

- Démarrez votre poste en appuyant plusieurs fois sur la touche (F2 ou Suppr ou touche Bios) pour arriver aux paramètres du bios.

- Désactivez le "Fast Boot" et démarrez sur la clé USB ou votre support bootable.

2. Conseils après l'installation

⚙ Update Kali

Vous devez mettre à jour et mettre à niveau toutes les dépendances de votre poste de travail pour éviter les erreurs d'application et vous assurer que vous disposez de la dernière version de tout ce qui est nécessaire au bon fonctionnement de votre système.

(root👽kali):~# *sudo apt-get clean*

(root👽kali):~# *sudo apt-get update*

(root👽kali):~# *sudo apt-get upgrade -y*

(root👽kali):~# *sudo apt-get dist-upgrade -y*

⚙ Install Git

Git est un système de contrôle de version populaire conçu pour gérer de très grands projets avec rapidité et efficacité. Il est utilisé pour de nombreux projets open source de haut niveau, notamment le noyau Linux.

(root👽kali): ~ # *install git*

⚙ Création de un ''low level user''

De nombreuses applications telles que le navigateur Chromium et le navigateur Tor ne doivent jamais être ouvertes ou utilisées en tant qu'utilisateur root. Ces applications s'appuient fortement sur des autorisations de bas niveau pour offrir un certain degré de sécurité. Il peut être avantageux pour certains utilisateurs de créer un compte d'utilisateur à faibles privilèges pour de telles activités.

⚙ Paramètres du bureau et des fichiers

C'est une évidence. Vous devez être en mesure de donner à votre poste de travail l'apparence que vous souhaitez et, pour cela, vous devez personnaliser votre bureau/desktop.

Vous pouvez éventuellement installer *gnome-tweak* qui est un gestionnaire de paramètres et de personnalisation de bureau gratuit pour le bureau Gnome.

(root👽kali):~# sudo apt install gnome-tweaks

(root👽kali):~# gnome-tweaks

⚙ Installer un ''terminal multiplexer''

Un multiplexeur est un émulateur de terminal en mosaïque qui nous permet d'ouvrir plusieurs sessions de terminal dans une seule fenêtre. Le principal avantage de cela est de pouvoir voir toutes nos sessions de terminal ouvertes en même temps et de ne pas superposer les fenêtres les unes sur les autres. Voici un exemple de multiplexeur.

Il existe de nombreux multiplexeurs remarquables. *Tilix est* une option open source et fiable.
Les alternatives incluent *tmux* et *screen*.

Tilix est disponible dans les référentiels APT de Kali et peut être installé à l'aide de la commande ci-dessous.

(root👽kali):~# apt-get install tilix

⚙ Installez Tor Browser

Maintenant que vous avez une excellente distribution Linux, il est temps que vous ayez aussi un excellent navigateur, et *Tor Browser* est la voie à suivre. Il a des paramètres de proxy intégrés pour garder votre présence en ligne et vos données privées anonymes.

(root👽kali):~# sudo apt install tor

⚙ Installez vos outils préférés

Si vous installez la version "*everything*" dans la plupart des cas, il n'y aura pas besoin de faire des installations supplémentaires.

En effet, cette image est destinée aux scénarios hors ligne, lorsque vous souhaitez utiliser Kali Linux dans un endroit dépourvu de connectivité réseau. L'image est énorme (plus de 9 Go), car elle contient déjà presque tous les outils de Kali. Il n'est disponible que pour l'architecture 64 bits et ne peut être téléchargé que via torrent.

3. Scan Réseau – nmap

> Site officiel: https://nmap.org/
> Documentation: https://nmap.org/docs.html

Nmap (« Network Mapper ») est un outil open source d'exploration réseau et d'audit de sécurité. Il a été conçu pour scanner rapidement de grands réseaux, mais il fonctionne aussi très bien sur une cible unique. Nmap innove en utilisant des paquets IP bruts (raw packets) pour déterminer quels sont les hôtes actifs sur le réseau, quels services (y compris le nom de l'application et la version) ces hôtes permettent, quels systèmes d'exploitation (et leurs versions) ils utilisent, quels types de dispositifs de filtrage/pare-feux sont utilisés, ainsi que des douzaines d'autres caractéristiques. Nmap est généralement utilisé pour les audits de sécurité mais de nombreux gestionnaires de systèmes et de réseau l'apprécient pour les tâches de routine comme les inventaires de réseau, la gestion des mises à jour programmées ou la surveillance des hôtes et des services actifs.

Exemple. Un scan Nmap représentatif

```
# nmap -A -T4 scanme.nmap.org
Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: li86-221.members.linode.com
Not shown: 995 closed ports
PORT     STATE    SERVICE     VERSION
22/tcp   open     ssh         OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
| ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
|_2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
80/tcp   open     http        Apache httpd 2.2.14 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
646/tcp  filtered ldp
1720/tcp filtered H.323/Q.931
9929/tcp open     nping-echo  Nping echo
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.39
OS details: Linux 2.6.39
Network Distance: 11 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
[Cut first 10 hops for brevity]
11  17.65 ms li86-221.members.linode.com (74.207.244.221)

Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds
```

Synopsis

(root👽kali):~# nmap [<Type de numérisation> ...] [<Options>] { <spécification cible> }

Le premier type de scan qui peut être utile, c'est le scan de machines.
Le permet de lister les machines disponibles sur le réseau, et de retourner leur IP, leur adresse MAC, et éventuellement leur nom d'hôte.

(root👽kali):~# nmap

Exemples d'utilisation

(root kali):~# *nmap nmap -v scanme.nmap.org*

Cette option analyse tous les ports TCP réservés sur la machine scanme.nmap.org . L'option -v active le mode ‘’verbose’’.

(root kali):~# nmap -sS -O scanme.nmap.org/24

Lance une analyse SYN furtive sur chaque machine parmi les 256 IP sur le réseau de taille /24 où réside Scanme. Il essaie également de déterminer quel système d'exploitation s'exécute sur chaque hôte en cours d'exécution. Cela nécessite des privilèges root en raison de l'analyse SYN et de la détection du système d'exploitation.

(root kali):~# nmap -sV -p 22,53,110,143,4564 198.116.0-255.1-127

Lance l'énumération des hôtes et une analyse TCP sur la première moitié de chacun des 255 sous-réseaux huit bits possibles dans l'espace d'adressage 198.116.0.0/16. Cela teste si les systèmes exécutent SSH, DNS, POP3 ou IMAP sur leurs ports standard, ou quoi que ce soit sur le port 4564. Pour l'un de ces ports trouvés ouverts, la détection de version est utilisée pour déterminer quelle application est en cours d'exécution.

(root kali):~# nmap nmap -v -iR 100000 -Pn -p 80

Demande à Nmap de choisir 100 000 hôtes au hasard et de les scanner pour les serveurs Web (port 80). L'énumération des hôtes est désactivée avec -Pn depuis le premier envoi de quelques sondes pour déterminer si un hôte est actif est un gaspillage lorsque vous ne sondez qu'un seul port sur chaque hôte cible de toute façon.

(root kali):~# nmap nmap -Pn -p80 -oX logs/pb-port80scan.xml -oG logs/pb-port80scan.gnmap 216.163.128.20/20

Cela analyse 4096 adresses IP pour tous les serveurs Web (sans leur envoyer de ping) et enregistre la sortie aux formats grepable et XML.

Nmap Scripting Engine (NSE)

Il est possible de créer différents scripts sur nmap.
Il existe une page sur github avec différents référentiels de scripts qui pourraient être utiles pour un objectif de test d'intrusion. → https://github.com/topics/nmap-scripts

En effet, le moteur de script Nmap (NSE) est l'une des fonctionnalités les plus puissantes et les plus flexibles de Nmap. Il permet aux utilisateurs d'écrire (et de partager) des scripts simples (en utilisant le langage de programmation Lua) pour automatiser une grande variété de tâches de mise en réseau. Ces scripts sont exécutés en parallèle avec la rapidité et l'efficacité que vous attendez de Nmap.

Les utilisateurs peuvent compter sur l'ensemble croissant et diversifié de scripts distribués avec Nmap, ou écrire les leurs pour répondre à des besoins personnalisés.

Les tâches que nous avions en tête lors de la création du système incluent la découverte du réseau, la détection de versions plus sophistiquées, la détection de vulnérabilité.
NSE peut même être utilisé pour l'exploitation de vulnérabilités.

Pour refléter ces différents usages et simplifier le choix des scripts à exécuter, chaque script contient un champ l'associant à une ou plusieurs catégories. Les catégories actuellement définies sont : auth, broadcast, default. découverte, dos, exploit, externe, fuzzer, intrusif, malware, safe, version et vuln.
Celles-ci sont toutes décrites dans la section intitulée “Catégories de scripts”.

Les scripts ne sont pas exécutés dans un “sandbox” et pourraient donc accidentellement ou malicieusement endommager votre système ou envahir votre vie privée. N'exécutez jamais de scripts de tiers à moins que vous ne fassiez confiance aux auteurs ou que vous n'ayez soigneusement vérifié les scripts vous-même.

Le moteur de script Nmap est décrit en détail ici → https://nmap.org/book/nse.html

Méthodologie d'analyse Intrusion WiFi

Vous voulez savoir si votre réseau Wi-Fi est facile à pirater ? En tant qu'utilisateur de Kali Linux, vous disposez de centaines d'outils d'audit de sécurité et de tests d'intrusion préinstallés. Ces outils sont destinés au piratage éthique - trouver et réparer les points faibles d'un réseau - et non à des fins illégales. Pour savoir si un réseau WPA/SPA PSK est sensible à une attaque par mot de passe par force brute, vous pouvez utiliser une suite d'outils appelée aircrack-ng pour pirater la clé. Nous allons vous montrer comment

Fern Wifi Cracker

Fern Wifi cracker est l'un des outils dont dispose Kali pour craquer sans fil.
Avant d'ouvrir Fern, nous devons activer la carte sans fil en mode de surveillance. Pour cela, tapez « ***airmon-ng start wlan-0*** » dans le terminal.
Généralement, dans les réseaux WPA, il effectue des attaques par dictionnaire en tant que telles.

Kismet

Kismet est un outil d'analyse de réseau WIFI. Il s'agit d'un détecteur de réseau sans fil 802.11 couche 2, d'un renifleur et d'un système de détection d'intrusion. Il fonctionne avec n'importe quelle carte sans fil prenant en charge le mode de surveillance brute (rfmon) et peut renifler le trafic 802.11a /b/g/n. Il identifie les réseaux en collectant des paquets et également des réseaux cachés.
Pour l'utiliser, mettez la carte sans fil en mode surveillance et pour cela, tapez « ***airmon-ng start wlan-0*** » dans le terminal.

GISKismet

GISKismet est un outil de visualisation sans fil pour représenter les données recueillies à l'aide de Kismet de manière pratique. GISKismet stocke les informations dans une base de données afin que nous puissions interroger les données et générer des graphiques à l'aide de SQL. GISKismet utilise actuellement SQLite pour la base de données et les fichiers GoogleEarth / KML pour les graphiques.

Ghost Phisher

Ghost Phisher est un outil populaire qui aide à créer de faux points d'accès sans fil, puis plus tard à créer Man-in-The-Middle-Attack.

Aircrack-ng

Aircrack-ng est un outil préinstallé dans Kali Linux et utilisé pour la sécurité et le piratage du réseau wifi. Aircrack est un renifleur de paquets tout-en-un, un cracker WEP et WPA / WPA2, un outil d'analyse et un outil de capture de hachage. C'est un outil utilisé pour le piratage wifi. Cela aide à capturer le paquet et à en lire les hachages et même à casser ces hachages par diverses attaques comme les attaques par dictionnaire. Il prend en charge presque toutes les dernières interfaces sans fil.
Il se concentre principalement sur 4 domaines :

- Surveillance : capture les fichiers cap, packet ou hash.
- Attaque : effectue une désauthentification ou crée de faux points d'accès
- Test : vérification des cartes Wi-Fi ou des capacités du pilote
- Cracking : diverses normes de sécurité telles que WEP ou WPA PSK.

Quelques commandes génériques

1. Pour répertorier toutes les interfaces réseau.
(root👽kali):~# airmon-ng

2. Arrêt de l'interface réseau souhaitée.
(root👽kali):~# airmon-ng stop [*nom interface wlan (generally wlan0)*

3. Démarrage d'une interface réseau sur un canal spécifique.
(root👽kali):~# *airmon-ng démarrer wlan0 [WiFi channel (for 2.4ghz network, 1 to 11]*

4. Pour accéder à la section d'aide de l'outil
(root👽kali):~# *aircrack-ng --help*

5. Pour afficher le nombre de processeurs et le support SIMD
(root👽kali):~# *aircrack-ng -u*

Exemples d'utilisation

WPA Wordlist Mode

Spécifiez la liste de mots à utiliser (-w password.lst) et le chemin d'accès au fichier de capture (wpa.cap) contenant au moins une 4-way handshake

```
root@kali:~# aircrack-ng -w password.lst wpa.cap
                              Aircrack-ng 1.5.2

      [00:00:00] 232/233 keys tested (1992.58 k/s)
      Time left: 0 seconds                                      99.57%

                           KEY FOUND! [ biscotte ]


      Master Key     : CD D7 9A 5A CF B0 70 C7 E9 D1 02 3B 87 02 85 D6
                       39 E4 30 B3 2F 31 AA 37 AC 82 5A 55 B5 55 24 EE

      Transient Key  : 33 55 0B FC 4F 24 84 F4 9A 38 B3 D0 89 83 D2 49
                       73 F9 DE 89 67 A6 6D 2B 8E 46 2C 07 47 6A CE 08
                       AD FB 65 D6 13 A9 9F 2C 65 E4 A6 08 F2 5A 67 97
                       D9 6F 76 5B 8C D3 DF 13 2F BC DA 6A 6E D9 62 CD

      EAPOL HMAC     : 28 A8 C8 95 B7 17 E5 72 27 B6 A7 EE E3 E5 34 45
```

Craquage WEP de base

Pour que aircrack-ng mène une attaque par clé WEP sur un fichier de capture, transmettez-lui le nom du fichier, au format .ivs ou .cap / .pcap :

```
root@kali:~# aircrack-ng all-ivs.ivs
                                  Aircrack-ng 1.4
                    [00:00:00] Tested 1514 keys (got 30566 IVs)

   KB    depth   byte(vote)
    0    0/  9   1F(39680) 4E(38400) 14(37376) 5C(37376) 9D(37376)
    1    7/  9   64(36608) 3E(36352) 34(36096) 46(36096) BA(36096)
    2    0/  1   1F(46592) 6E(38400) 81(37376) 79(36864) AD(36864)
    3    0/  3   1F(40960) 15(38656) 7B(38400) BB(37888) 5C(37632)
    4    0/  7   1F(39168) 23(38144) 97(37120) 59(36608) 13(36352)

                          KEY FOUND! [ 1F:1F:1F:1F:1F ]
    Decrypted correctly: 100%
```