PIRATÉ

GUIDE ULTIME DE KALI LINUX ET DE HACKING SANS FIL AVEC DES OUTILS DE TEST DE SÉCURITÉ ET DE PÉNÉTRATION, LIVRE PRATIQUE DE HACKING D'ORDINATEUR ÉTAPE PAR ÉTAPE

TEKTIME

ALAN T. NORMAN

Alan T. Norman

Piraté

«Tektime S.r.l.s.»

Norman A.

Piraté / A. Norman — «Tektime S.r.l.s.»,

Le livre de piratage est destiné à servir de guide de niveau intermédiaire à certains outils et compétences de test de pénétration courants, en particulier ceux du piratage sans fil et du maintien de l'anonymat. Le livre se concentre davantage sur l'exécution pratique et fournit des procédures étape par étape pour l'installation des plates-formes et des outils essentiels, ainsi que la théorie derrière certaines attaques de base. Acquérez la possibilité de faire du piratage éthique et des tests de pénétration en prenant ce livre sur le piratage! Le livre de piratage est destiné à servir de guide de niveau intermédiaire à certains outils et compétences de test de pénétration courants, en particulier ceux du piratage sans fil et du maintien de l'anonymat. Le livre se concentre davantage sur l'exécution pratique et fournit des procédures étape par étape pour l'installation des plates-formes et des outils essentiels, ainsi que la théorie derrière certaines attaques de base. Acquérez la possibilité de faire du piratage éthique et des tests de pénétration en prenant ce livre sur le piratage! Obtenez des réponses d'un expert informatique expérimenté à chaque question que vous avez liée à l'apprentissage que vous faites dans ce livre, y compris: - l'installation de Kali Linux en utilisant les bases de VirtualBox de Linux Rester anonyme avec Tor Proxychains, - Virtual Private Networks (VPN) Macchanger, - Nmap cracking wifi aircrack craquer les mots de passe Linux Quelles sont les exigences? Connexion Internet fiable et rapide. Carte réseau sans fil. Kali Linux Distribution Compétences informatiques de base Que retirerez-vous du livre sur le piratage? Réponses à chaque question que vous vous posez sur le piratage éthique et les tests d'intrusion par un professionnel de l'informatique expérimenté! Vous apprendrez les bases du réseau Traitez avec de nombreux outils Kali Linux Apprenez quelques commandes Linux Conseils pour rester anonyme dans les activités de piratage et de test de pénétration. Protégez votre réseau WiFi contre toutes les attaques Accédez à n'importe quel compte client du réseau WiFi Un tutoriel complet expliquant comment créer un environnement de piratage virtuel, attaquer les réseaux et casser les mots de passe. Instructions étape par étape pour l'isolation de VirtualBox et la création de votre environnement virtuel sur Windows, Mac et Linux.

Содержание

Piraté

Guide Ultime De Kali Linux Et De Hacking Sans Fil Avec Des Outils De Test De Sécurité Et De Pénétration, Livre Pratique De Hacking D'ordinateur Étape Par Étape

Alan T. Norman

Traducteur : Ilyasse Kourriche

Avis de non-responsabilité :

Veuillez noter que les informations contenues dans ce document ne sont pas destinées à des fins éducatives et de divertissement. Tout a été fait pour fournir des informations complètes, exactes, à jour et fiables. Aucune garantie de quelque nature que ce soit n'est exprimée ou implicite.

En lisant ce document, le lecteur accepte qu'en aucun cas l'auteur ne soit responsable des pertes, directes ou indirectes, qui sont encourues suite à la publication des informations contenues dans ce document, y compris, mais sans s'y limiter, les erreurs, omissions ou inexactitudes

Table of Contents

Introduction

Ce livre est destiné à servir de guide de niveau intermédiaire pour certains outils et compétences courants en matière de tests de pénétration - en particulier ceux du piratage sans fil et du maintien de l'anonymat. Le matériel est basé sur les informations de base fournies dans le livre Hacking for Beginners, il suppose donc que le lecteur a une certaine familiarité avec les concepts et la terminologie du hacking pour débutants. Contrairement à Hacking for Beginners, ce livre se concentre davantage sur l'exécution pratique et fournit des procédures étape par étape pour l'installation de plateformes et d'outils essentiels, ainsi que la théorie derrière certaines attaques de base.

LES "QUATRE GRANDS"

Il y a quatre domaines principaux que tous les pirates informatiques devraient considérer et affiner, quel que soit leur niveau de compétence. Si vous voulez devenir un maître du piratage informatique, vous devez constamment travailler à vous améliorer dans ces quatre domaines. Ces "quatre grands" sont les connaissances, les outils, les compétences et le jugement. En lisant ce livre et en mettant ses idées en pratique, vous devez vous demander lesquels de ces domaines sont pertinents pour le concept en question. Cela vous aidera à créer un cadre pour vos capacités et à suivre vos progrès au fur et à mesure.

CONNAISSANCES

Une connaissance approfondie et large des concepts pertinents est la base de tout hacker qui réussit. L'acquisition de connaissances n'est pas seulement le début d'une carrière de hacker, mais doit être constamment entretenue en raison de la rapidité avec laquelle l'information se développe et évolue dans le monde informatique. Il existe une offre apparemment inépuisable de sources de connaissances et de domaines d'études, à tel point qu'il est probablement impossible de tout connaître. Cependant, il est essentiel de se consacrer à la recherche constante de connaissances. Il existe plusieurs domaines sur lesquels il faut se concentrer et qui sont essentiels pour une base de connaissances opérationnelle en matière de sécurité et d'exploitation informatique. Dans l'ordre successif, ils le sont généralement :

Architecture des ordinateurs et des réseaux
Protocoles de mise en réseau
Sécurité de l'information et des réseaux
Programmation informatique
Cryptage des données
Vulnérabilités des logiciels et du matériel
Anonymisation
Exploitation

Ces domaines de connaissance se chevauchent dans certains cas et le lecteur n'est certainement pas limité à la liste ci-dessus (plus il y a de connaissances, mieux c'est !), mais elle représente une bonne liste de "choses à faire" pour les autodidactes. Des informations dans tous ces domaines peuvent être trouvées dans des livres, des ebooks, des journaux, des sites web, des cours en ligne et hors ligne, des mentors personnels et des conférences, entre autres sources. Il peut être utile, si cela est abordable, de devenir diplômé ou certifié en réseau, en programmation ou en sécurité de l'information.

OUTILS

La connaissance est inutile sans les outils permettant de l'exploiter. Le hacker a besoin d'un ensemble de base d'outils matériels et logiciels qui restent fondamentalement les mêmes quel que soit son niveau de compétence. Ces outils s'accumuleront et évolueront au fil du temps, au fur et à mesure des progrès technologiques et de la défense. Les trois catégories d'outils de base nécessaires à un hacker qui réussit sont les suivantes

Une plate-forme matérielle telle qu'un ordinateur portable ou de bureau, ou un appareil mobile

Appareils de mise en réseau tels que les cartes d'interface et les adaptateurs sans fil

Logiciels tels que les systèmes d'exploitation (y compris les machines virtuelles), les kits de développement, les applications de surveillance du réseau, les scripts et les paquets d'exploitation

La plupart des outils ne sont pas particulièrement sophistiqués, coûteux ou difficiles à obtenir. Les ordinateurs peuvent être chers, mais la plupart des opérations de piratage ne nécessitent pas la machine la plus récente et la plus rapide du marché. Pour la plupart des procédures, un ordinateur portable disposant d'une quantité raisonnable de mémoire et pouvant supporter des systèmes d'exploitation modernes est généralement suffisant. Bien que la plupart des ordinateurs soient équipés en standard de matériel de réseau, la pénétration du Wi-Fi nécessite un type spécial de puce sans fil (voir chapitre 10) qui n'est généralement pas fourni avec les adaptateurs standard. Un adaptateur USB externe doté de cette caractéristique peut cependant être obtenu à un prix relativement bas.

La quasi-totalité des logiciels nécessaires aux procédures de piratage les plus courantes sont gratuits, open-source et faciles à obtenir. Ces outils peuvent être téléchargés librement et sont fréquemment mis à jour. La plupart de ces outils sont soutenus par une riche communauté d'utilisateurs enthousiastes qui constituent une excellente ressource pour les conseils et le dépannage. Il est important pour les pirates de maintenir leurs logiciels à jour avec les dernières versions et les derniers correctifs et de surveiller la communauté pour les problèmes actuels, les solutions et les cas d'utilisation.

COMPETENCES

Les compétences des pirates informatiques sont acquises lorsque les connaissances et les outils sont réunis pour atteindre un objectif. En fin de compte, les compétences d'un hacker déterminent ce qu'il peut ou ne peut pas accomplir. Une fois que l'on dispose de connaissances et d'outils, la construction d'un bon ensemble de compétences nécessite une chose... la pratique.

Les compétences peuvent être pratiquées en toute sécurité dans un environnement autonome tel qu'un réseau local ou un réseau personnel, ou dans un ensemble de machines virtuelles en réseau au sein d'un même système. En outre, il existe un certain nombre de sites web, gratuits ou payants, où les pirates et les professionnels de la sécurité peuvent pratiquer des méthodes offensives et défensives dans un espace sans conséquences.

Comme toute autre compétence, les compétences en matière de piratage informatique diminueront si elles ne sont pas utilisées, que ce soit avec de la pratique ou de l'application, de manière régulière. En outre, vous ne pouvez jamais supposer qu'une fois qu'une compétence est apprise, elle reste utilisable pour toujours. La nature du piratage et de la sécurité est telle qu'elle évolue constamment et rapidement. Il fut un temps, par exemple, où l'injection SQL était une attaque simple et courante sur les sites web, mais maintenant que les administrateurs ont compris (et que le code côté serveur est devenu plus sûr), on considère qu'elle est dépassée. Une vulnérabilité récente a été découverte dans les réseaux Wi-Fi (voir chapitre 11) qui est maintenant à la pointe du progrès. Pour rester efficace, il faut rafraîchir les compétences avec les connaissances et les outils les plus récents.

JUGEMENT

Enfin, et c'est peut-être le plus important, un hacker doit toujours faire preuve d'un jugement sûr. Alors que les compétences déterminent ce qu'un hacker peut faire, le jugement détermine ce qu'il doit faire. Une grande partie des connaissances et des compétences requises pour le hacking implique la compréhension de plusieurs concepts avancés. Bien que la société moderne soit très avancée techniquement, la plupart des personnes que vous rencontrez dans la vie quotidienne n'ont qu'une fraction des connaissances requises pour comprendre, et encore moins pour exécuter, même le plus simple des piratages. Les hackers font ainsi partie d'un club assez exclusif, donnant au novice un sentiment enivrant de puissance et d'invincibilité. Mais à côté de toutes les connaissances techniques qui accompagnent l'étude du piratage, il faut aussi comprendre les différents risques et conséquences. Il est tentant de vouloir d'abord sauter dans les pieds et de pratiquer ses nouvelles compétences, mais toutes les actions doivent d'abord être tempérées par des questions sobres.

Un hacker doit avoir des objectifs clairs à l'esprit avant de se lancer dans une quelconque entreprise, même si elle n'est destinée qu'à la pratique. Toutes les actions doivent être entreprises en tenant dûment compte de ses propres normes éthiques, des attentes de la communauté et des conséquences potentielles (voir le dilemme dans la Figure 1). Une erreur courante pour les débutants est de surestimer leur niveau d'anonymat. Une erreur encore plus grave est de surestimer son niveau de compétence. Une attaque mal exécutée peut révéler l'identité du hacker ou causer des dommages involontaires ou la perte de données dans un système cible. Il faut du temps pour atteindre un niveau de compétence approprié pour n'importe quelle tâche, et l'impatience peut tout gâcher.

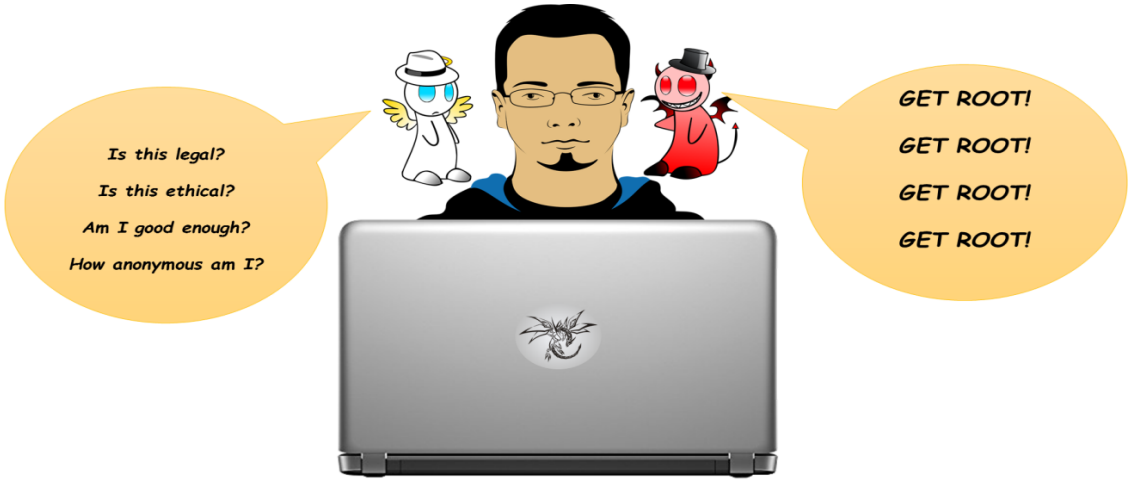

Figure 1 - Le dilemme du hacker

Quelques Mots De Prudence

Avant de se lancer dans une mission de test de pénétration, ou de mettre en œuvre de toute autre manière les connaissances et les compétences acquises dans ce livre, le lecteur doit garder à l'esprit les conseils de prudence suivants.

Un Paysage En Mutation Rapide

Plus que tout autre type d'industrie ou de technologie, le monde des ordinateurs et des réseaux d'information (tant en termes de matériel que de logiciels) est en pleine mutation. De nouvelles versions - parfois même plusieurs versions en avance - sont toujours en production avant même que les plus récentes n'arrivent sur le marché. Il n'est généralement pas possible de prévoir quand une nouvelle version, sous-version ou correctif sera publié pour un paquet donné - ou quels changements viendront avec cette publication. Le monde des logiciels à source ouverte, d'où proviennent la plupart des outils de piratage, est particulièrement chaotique. Les versions, les correctifs et la documentation sont souvent réalisés par la communauté des utilisateurs et ne sont pas nécessairement maintenus de manière centralisée par un contrôle de qualité rigoureux. Il existe plusieurs types de distributions pour les systèmes d'exploitation à source ouverte et d'autres outils, et elles ne coordonnent pas toujours les changements apportés à leur code de base. En raison de ce paysage en évolution rapide et souvent imprévisible, toute étape individuelle ou syntaxe de commande donnée pour une procédure particulière est susceptible d'être modifiée à tout moment. En outre, la mise en œuvre de certaines procédures peut varier, parfois de manière subtile et parfois de manière drastique, en fonction de la nature du matériel ou du système d'exploitation sur lequel elles fonctionnent.

Ce livre tente de présenter les informations les plus récentes, les plus courantes et les plus universelles, et il fournit des mises en garde lorsque les procédures sont connues pour être différentes. Toutefois, le lecteur doit être conscient du fait que la mise en œuvre de nombreuses procédures présentées dans ce livre s'accompagne souvent d'un grand nombre de dépannages et d'affinements des différentes étapes. Lorsque des erreurs ou des résultats inattendus se produisent, il existe sur Internet des ressources gratuites permettant d'obtenir des informations actualisées. Les meilleurs endroits à consulter sont les sites web des hôtes des logiciels en question, et les divers forums de discussion des pirates informatiques ou des logiciels. Dans la plupart des cas, quelqu'un d'autre a déjà trouvé et publié une solution au problème que vous rencontrez.

Les Limites De L'anonymat

Ce livre présente plusieurs outils et méthodes permettant aux pirates informatiques (ou même aux simples internautes) de conserver un certain anonymat. Ces procédures vont de la dissimulation ou de l'obscurcissement de l'adresse IP ou MAC d'une personne à l'accès aux ressources par des canaux cryptés ou à sauts multiples. Cependant, il est important de comprendre que la nature de la communication rend pratiquement impossible pour quiconque de maintenir un anonymat à 100 %. Une partie motivée et bien financée, qu'il s'agisse d'une organisation criminelle ou gouvernementale (ou des deux, dans certains cas) peut très souvent déterminer les informations qu'elle recherche.

Dans de nombreux cas, il suffit d'une seule erreur mineure de la part de la personne qui souhaite rester anonyme pour révéler son emplacement ou son identité. La nature des activités de cette personne déterminera généralement les ressources que d'autres personnes sont prêtes à consacrer pour la retrouver. Il est toujours possible de maintenir un degré élevé de confiance dans son anonymat en mettant correctement en œuvre plusieurs méthodes simultanément. Dans de nombreux cas, cela rendra le temps nécessaire pour retrouver une personne prohibitif et coûteux. En fin de compte, vous ne devez jamais supposer que vous êtes totalement sûr ou anonyme.

Conséquences Juridiques Et Éthiques

Hacking for Beginners présente une analyse détaillée des différentes questions juridiques et éthiques qui doivent être prises en compte avant d'entreprendre le piratage informatique comme passe-temps ou carrière. Ce livre présente les informations de manière factuelle et encourage l'utilisateur à utiliser les connaissances acquises avec soin et diligence. Aucun des outils ou procédures décrits dans ce livre n'est illégal ou même contraire à l'éthique lorsqu'il est utilisé dans le bon contexte. En fait, ils sont essentiels pour comprendre la nature des menaces modernes à la sécurité de l'information et pour s'en protéger. En outre, il est courant et conseillé de mener des attaques contre ses propres systèmes afin d'identifier et de corriger les vulnérabilités. Tenter d'accéder à un système ou de le compromettre sans l'autorisation de son propriétaire n'est pas recommandé, surtout pour les débutants inexpérimentés, et pourrait entraîner de graves conséquences, y compris des poursuites pénales. Assurez-vous de bien comprendre les lois et les sanctions - qui peuvent varier selon le pays et la localité - et, comme mentionné ci-dessus, ne comptez pas sur l'anonymat pour vous protéger.

Chapitre 1. Kali linux

Pour se lancer dans le piratage sans fil, il faut d'abord se familiariser avec les outils du métier. Aucun outil n'est plus précieux, surtout pour un hacker débutant, que Kali Linux. Ensemble de logiciels d'analyse et de pénétration gratuits, stables, bien entretenus et étonnamment complets, Kali a évolué dans le creuset des distributions Linux à source ouverte et s'est imposé comme le roi de tous les systèmes d'exploitation pour hackers. Ce successeur de la célèbre distribution BackTrack possède tout ce dont un hacker a besoin, des débutants aux experts aguerris.

Une Brève Histoire D'unix Et De Linux

Au début des années 1970, le système d'exploitation Unix - abrégé en UNICS (UNiplexed Information and Computing Service) - est issu d'un projet défunt d'AT&T Bell Labsto qui permettait aux utilisateurs d'accéder simultanément aux services informatiques centraux. Avec la formalisation et la popularité croissante d'Unix, il a commencé à remplacer les systèmes d'exploitation natifs sur certaines plates-formes mainframe courantes. Écrit à l'origine en langage assembleur, la réécriture d'Unix en langage de programmation C a amélioré sa portabilité. Finalement, plusieurs versions d'Unix, y compris celles pour les micro-ordinateurs, ont émergé sur le marché commercial. Plusieurs dérivés de systèmes d'exploitation populaires, appelés "Unix-like", ont pris forme dans les décennies suivantes, notamment le système d'exploitation Mac d'Apple, Solaris de Sun Microsystem et BSD (Berkeley Software Distribution).

Les efforts pour créer une version librement disponible d'Unix ont commencé dans les années 1980 avec le projet de licence publique générale (GPL) de GNU ("GNU's Not Unix"), mais n'ont pas réussi à produire un système viable. Cela a conduit le programmeur finlandais Linus Torvalds à s'attaquer au développement d'un nouveau noyau Unix (le module de contrôle central d'un système d'exploitation) en tant que projet étudiant. En utilisant le système d'exploitation éducatif Minix, similaire à Unix, Torvalds a codé avec succès un noyau de système d'exploitation en 1991, rendant le code source librement disponible pour le téléchargement et la manipulation publique sous la licence GNU GPL. Le projet a finalement été nommé Linux (une combinaison du prénom de Torvalds, "Linus", avec "Unix").

Bien que le terme Linux se réfère initialement uniquement au noyau développé par Torvalds, il en est venu à désigner tout ensemble de systèmes d'exploitation basé sur le noyau Linux. Étant un effort d'open-source, diverses distributions de Linux ont évolué au cours des décennies avec des ensembles uniques de bibliothèques logicielles, de pilotes de matériel et d'interfaces utilisateur. La flexibilité et l'efficacité de Linux ont conduit à une large adoption par les passionnés d'informatique et certaines grandes organisations, à la fois par mesure d'économie et pour contourner le monopole de Microsoft sur les systèmes d'exploitation.

Comme la plupart des logiciels grand public et professionnels populaires sont écrits pour les plates- formes Microsoft et Apple, Linux n'a jamais eu l'omniprésence ou l'attrait commercial des systèmes d'exploitation Windows et Macintosh pour PC. Cependant, la flexibilité, la portabilité et la nature open-source de Linux en font un outil idéal pour la création de distributions légères et très personnalisées qui répondent à des besoins très spécifiques. Ces distributions sont généralement construites à partir du noyau - en n'installant que les bibliothèques et les composants minimums nécessaires pour atteindre les objectifs du matériel hôte. Cette approche produit des paquets de systèmes d'exploitation qui utilisent un minimum de mémoire, de stockage et de ressources processeur et présentent moins de vulnérabilités en matière de sécurité. Linux, ainsi que la syntaxe et la structure Unix sur lesquelles il est basé, est une partie essentielle de la boîte à outils et de la base de connaissances d'un hacker moderne.

Des centaines de distributions Linux individuelles commerciales et à code source ouvert ont vu le jour et fonctionnent actuellement sur tout, des petits appareils personnels tels que les téléphones et les montres intelligentes aux ordinateurs personnels, aux serveurs centraux et au matériel militaire. La plupart de ces distributions se sont dérivées d'une poignée de paquets Linux antérieurs, dont Debian, Red Hat et SLS.

Debian Linux Et Knoppix

Debian, l'un des premiers projets de distribution Linux ouverte, a été consciemment créé pour rester libre et ouvert tout en maintenant des normes de qualité élevées. Debian a eu plusieurs distributions majeures de son propre chef, en plus de douzaines de projets dérivés qui utilisent le noyau et la base de bibliothèques de Debian. Alors que deux de ces projets, Linspire et Ubuntu (une distribution très populaire) étaient principalement destinés aux utilisateurs de PC domestiques, le projet Knoppix a été conçu pour être exécuté en direct à partir d'un support externe, tel qu'un CD-ROM. Cela - ainsi que sa capacité à s'interfacer avec un large éventail de matériel - a fait de Knoppix un outil idéal pour le dépannage, le sauvetage de données, la récupération de mots de passe et d'autres opérations utilitaires.Knoppix a été une base naturelle à partir de laquelle ont été développées les différentes sous-distributions de sécurité, de tests de pénétration et de médecine légale qui ont ensuite vu le jour.

Retour Sur Linux

Deux distributions basées sur Debian Knoppix qui se sont concentrées sur les tests de pénétration étaient WHAX (anciennement Whoppix) et l'Auditor Security Collection. Les deux projets fonctionnaient sur des CD en direct et comportaient un important dépôt d'outils de tests de pénétration. WHAX et Auditor Security ont finalement fusionné dans la fameuse distribution connue sous le nom de BackTrack.

Kali Linux

La suite complète de sécurité offensive et défensive incluse dans BackTrack Linux en a fait l'outil de choix pour les amateurs, les professionnels de la sécurité, les testeurs de pénétration légitimes et les pirates informatiques. Le développeur de BackTrack, Offensive Security, a finalement réécrit la distribution, en renommant le projet Kali Linux. Les paquets d'installation de Kali et les images des machines virtuelles sont disponibles gratuitement. Offensive Security propose également des cours payants sur la sécurité avec Kali, ainsi que des certifications professionnelles et un environnement de test d'intrusion en ligne.

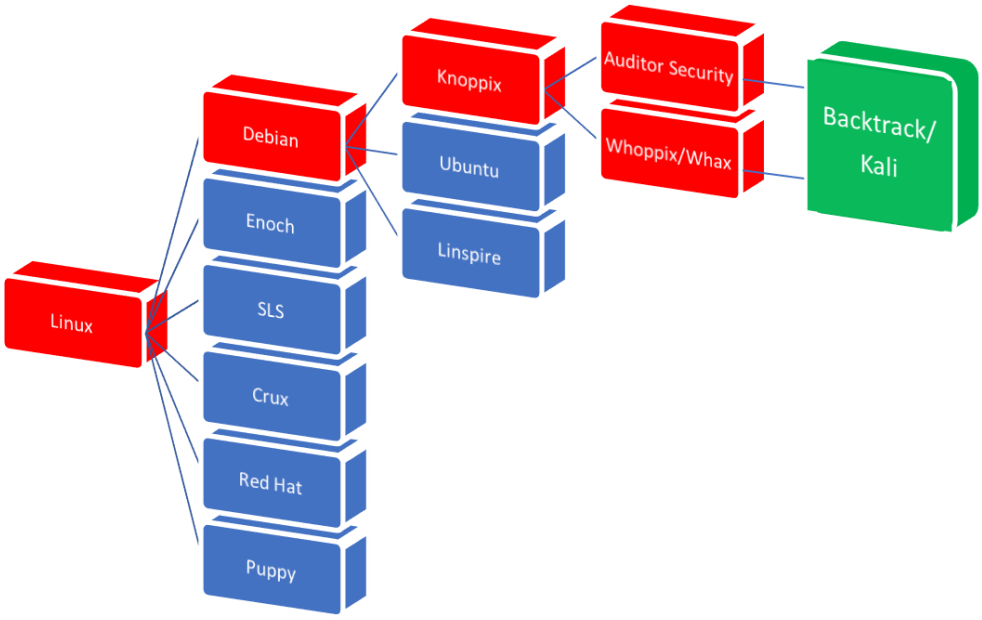

Figure 2 - Évolution de Kali Linux

OUTILS KALI

La pièce maîtresse de Kali Linux, et la raison principale de sa popularité auprès des pirates et des professionnels de la sécurité, est sa suite d'outils gratuits, vaste et bien organisée. Kali propose actuellement plus de 300 outils, dont la collecte passive d'informations, l'évaluation des vulnérabilités, la criminalistique, le craquage de mots de passe, l'analyse de réseau, le piratage sans fil et un ensemble puissant d'outils d'exploitation. Bien que tous les outils inclus dans Kali soient gratuits et à code source ouvert et puissent être téléchargés et intégrés à la plupart des dérivés de Linux (basés sur Debian), disposer d'un système d'exploitation testé et approuvé, livré en natif avec un tel ensemble d'outils, est une ressource inestimable.

Parmi les outils les plus utiles qui accompagnent Kali, on trouve

MetasploitFramework-Metasploit est une plateforme populaire d'exploitation des vulnérabilités contenant divers outils d'analyse et de pénétration. Elle propose de multiples options d'interface utilisateur et offre à l'utilisateur la possibilité d'attaquer presque tous les systèmes d'exploitation. Kali contient également Armitage, une plate-forme de gestion graphique qui aide l'utilisateur à organiser les opérations et les interactions entre les différents outils Metasploit lors d'une attaque.

Wireshark - Wireshark est un outil multi-plateforme d'analyse du trafic réseau en temps réel. Tout le trafic sur un nœud de réseau choisi est capturé et décomposé en métadonnées de paquets utiles,

y compris l'en-tête, les informations de routage et la charge utile. Wireshark peut être utilisé pour détecter et analyser les événements de sécurité du réseau et pour dépanner les défaillances du réseau.

John the Ripper - John the Ripper est un outil légendaire de craquage de mots de passe contenant de multiples algorithmes d'attaque de mots de passe. Bien qu'il ait été initialement écrit exclusivement pour Unix, John the Ripper est maintenant disponible sur plusieurs plates-formes de systèmes d'exploitation. L'une de ses caractéristiques les plus utiles est sa capacité à détecter automatiquement le type de cryptage de mot de passe "hash". La version gratuite de John the Ripper disponible sur Kali permet de craquer de nombreux algorithmes de hachage de mots de passe, mais pas autant que son homologue commercial.

Nmap- Nmap, abréviation de network map ou network mapper, est un outil de piratage courant qui est essentiel pour les tests de pénétration. Nmap permet à l'utilisateur de scanner un réseau pour tous les hôtes et services réseau connectés, en fournissant une vue détaillée de la structure et des membres du réseau. En outre, Nmap fournit une liste des systèmes d'exploitation installés sur chaque hôte ainsi que de ses ports ouverts. Cela permet à l'utilisateur de se concentrer sur les vulnérabilités connues pendant l'exploitation.

Aircrack-ng - Aircrack-ng est le progiciel par excellence pour l'analyse et les tests de pénétration des réseaux sans fil. Il se concentre sur les protocoles de cryptage WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) et WPA2-PSK Wi-Fi. Cet outil comprend des outils de reniflage de paquets sans fil, d'injection de paquets, d'analyse de réseaux sans fil et de craquage de mots de passe cryptés. Le craquage nécessite un matériel d'interface réseau qui prend en charge la fonctionnalité du mode surveillance. Kali dispose également d'un outil de piratage sans fil plus graphique, appelé Fern.

BurpSuite-BurpSuite est une collection d'outils qui se concentre sur l'exploitation des applications web. Ces programmes interagissent non seulement pour tester les vulnérabilités des applications, mais aussi pour lancer des attaques.

La liste ci-dessus n'est en aucun cas complète, mais elle constitue un échantillon représentatif de la puissance et de la flexibilité que Kali Linux offre en tant que plateforme pour les tests d'intrusion et pour la sécurité informatique en général. Kali peut être exécuté en direct à partir d'un support optique ou USB, en tant que système d'exploitation autonome sur un poste de travail de bureau ou portable, comme alternative dans un système multiboot, ou dans une machine virtuelle à l'intérieur d'un autre système d'exploitation hôte. Le chapitre suivant décrit comment installer et configurer Kali sur différents systèmes d'exploitation afin de créer un environnement approprié pour le piratage et les tests de pénétration.

Конец ознакомительного фрагмента.