جامعة محمد الأول بوجدة
UNIVERSITE MOHAMMED PREMIER OUJDA

المدرسة الوطنية للعلوم التطبيقية
École Nationale des Sciences Appliquées

UNIVERSITE MOHAMMED PREMIER

ECOLE NATIONALE DES SCIENCES APPLIQUÉES OUJDA

Filière : Sécurité Informatique et Cyber Sécurité

Soutenu le : 01/07/2024

Rapport de Projet de Fin d'Année

Sous le thème :

Comparaison des outils de sécurité dans Kali Linux et Parrot OS et proposition d'une panoplie personnalisée

Réalisé par :

- AMAHROUK ASMAE
- IJFIRI MARIEME

Encadré par :

- Pr. JABRI Youssef

Membre de jury :

- Pr. REGAD Youssef

Année universitaire

2023-2024

Table de matières

Table de figures

Liste des tableaux

Remerciement

Nous tenons à exprimer notre sincère gratitude à toutes les personnes qui ont contribué à la réalisation de ce projet de fin d'année.

Tout d'abord, nous remercions chaleureusement notre professeur et superviseur, **Mr JABRI Youssef**, pour son encadrement et ses conseils précieux tout au long de ce projet. Son expertise et sa disponibilité ont été indispensables pour mener à bien ce travail.

Ainsi nous tenons à remercier **Pr. REGAD Youssef**, membre de jury, pour le temps et l'attention qu'il a consacré pour évaluer notre projet.

Nous tenons à exprimer notre profonde gratitude à nos camarades de classe, dont le soutien, la collaboration et l'amitié ont été essentiels à la réalisation de ce rapport.

Enfin, nous exprimons notre profonde gratitude à nos familles pour leur compréhension et leur soutien constant.

Un grand merci à tous ceux qui ont, de près ou de loin, contribué à la réussite de ce projet.

Résumé

Ce projet propose une étude comparative entre les outils de sécurité disponibles dans deux distributions Linux populaires axées sur la sécurité, **Kali Linux** et **Parrot OS**. Ces deux distributions sont largement utilisées par les professionnels ainsi que les débutant de la sécurité informatique pour le pentesting et d'autres tâches liées à la cybersécurité.

L'objectif principal du projet est d'analyser les différences et similitudes entre les outils de sécurité offerts par ces deux systèmes, en évaluant leurs fonctionnalités, performances et convivialité.

En plus de cette comparaison, le projet propose une panoplie personnalisée d'outils de sécurité, combinant les meilleures fonctionnalités des deux distributions et en se basant sur une variété de critères spécifiques, afin de fournir une solution optimale adaptée à divers scénarios de sécurité.

Puis, intègre les outils de la panoplie personnalisée dans un système basé sur Debian, notamment **Ubuntu 23.10**, à l'aide de **Katoolin3**.

Enfin, ce projet offre une analyse exhaustive et pratique des outils de sécurité dans **Kali Linux** et **Parrot OS**, guidant les utilisateurs vers une utilisation optimale des ressources disponibles pour la cybersécurité. Et il vient avec deux autres fichiers Excel, un contenant la panoplie personnalisée en fournissant la méthode d'installation de chaque outil sur les systèmes bases sur Debian, et un autre contenant l'étude comparative entre les outils de sécurité de Kali Linux et Parrot OS en détails selon les catégories et les sous-catégories.

Introduction générale

Dans notre monde de plus en plus connecté et dépendant de la technologie, la sécurité informatique est devenue un enjeu essentiel. Protéger nos données et nos systèmes contre les menaces numériques est désormais une priorité absolue. Dans ce contexte, des distributions Linux spécialisées dans la sécurité telles que **Kali Linux** et **Parrot OS** offrent une multitude d'outils et de fonctionnalités conçus pour aider les professionnels de la sécurité informatique dans leur mission.

Ce projet se propose d'explorer et de comparer les outils de sécurité intégrés dans **Kali Linux** et **Parrot OS,** deux distributions populaires largement utilisées dans la communauté de la sécurité informatique. Notre objectif est de comprendre les différences et les similitudes entre ces deux distributions, en examinant leurs fonctionnalités, leur performance et leur convivialité.

En outre, ce rapport vise à proposer une approche personnalisée en identifiant les outils les plus adaptés à différents scénarios de sécurité et en proposant une panoplie personnalisée d'outils de sécurité, combinant les meilleures fonctionnalités de **Kali Linux** et **Parrot OS.** Cette approche permettra aux utilisateurs de bénéficier d'une solution sur mesure, répondant efficacement à leurs besoins spécifiques en matière de sécurité informatique.

À travers cette étude comparative et cette proposition de panoplie personnalisée, nous espérons fournir aux professionnels de la sécurité informatique et aux passionnés des ressources précieuses pour renforcer la protection de leurs systèmes et de leurs réseaux dans un environnement numérique en constante évolution.

Chapitre 1 : Introduction aux distributions Kali Linux et Parrot OS

1. Distribution Kali Linux

1.1. Introduction

Kali Linux est une distribution Linux spécialisée dans les tests de pénétration et la sécurité informatique, souvent utilisée par des experts en cybersécurité pour évaluer la sécurité des systèmes et des réseaux. Cette distribution est le successeur direct de **BackTrack**, une autre distribution axée sur la sécurité qui a été largement utilisée jusqu'en 2013.

L'origine de **Kali Linux** remonte à la décision de transformer **BackTrack** en une distribution plus structurée et robuste. Les développeurs ont choisi de reconstruire la distribution sur la base de **Debian**, un choix qui a permis d'améliorer la gestion des paquets et la stabilité générale du système. Ce changement a également rendu **Kali Linux** plus accessible aux utilisateurs qui étaient déjà familiers avec Debian ou des distributions similaires.

Kali Linux est développé par **Offensive Security**, une entreprise renommée dans le domaine de la sécurité informatique. L'entreprise est également connue pour ses formations en cybersécurité, notamment le cours **Certified Ethical Hacker (CEH)** qui utilise **Kali Linux** comme une ressource clé dans le cadre de la formation pratique.

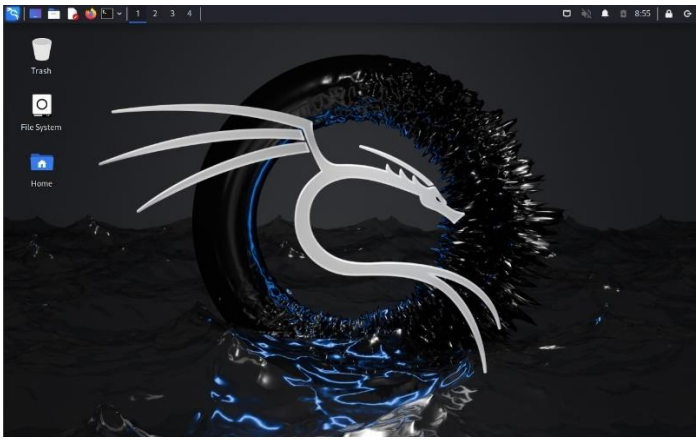

Figure 1 : *Kali Linux Distribution*

1.2. Architecture et Caractéristiques Techniques

1.2.1. Basé sur Debian

L'utilisation de Debian comme base pour **Kali Linux** est un choix stratégique crucial qui apporte plusieurs avantages majeurs, notamment en termes de stabilité, de sécurité et de gestion des paquets.

- **Stabilité** : Debian est renommée pour sa fiabilité. En tant que distribution, elle subit des tests rigoureux et une période de développement prolongée avant chaque nouvelle version stable. Cette stabilité est essentielle pour **Kali Linux**, car les professionnels de la

sécurité dépendent de l'environnement système pour fonctionner sans interruption et de manière prévisible pendant leurs tests de pénétration et audits.

- **Sécurité** : Debian met un point d'honneur à offrir un système d'exploitation sécurisé. Elle dispose d'une équipe dédiée à la sécurité qui s'assure que toutes les failles et vulnérabilités sont rapidement identifiées et corrigées. Pour une distribution comme **Kali Linux**, qui est utilisée dans des environnements où la sécurité est une priorité absolue, bénéficier de cette expertise en matière de sécurisation du système d'exploitation est fondamental.
- **Gestion de paquets** : Debian utilise le système de gestion de paquets **APT** (Advanced Package Tool), qui est l'un des systèmes de gestion de paquets les plus robustes et les mieux établis. Il permet une installation facile et une maintenance des logiciels. Pour Kali Linux, qui intègre des centaines d'outils spécifiques à la sécurité, le système **APT** permet aux utilisateurs de gérer facilement ces outils, de les mettre à jour ou de les remplacer. Ceci est crucial pour maintenir l'intégrité du système et s'assurer que les outils sont toujours à jour avec les dernières mesures de sécurité et fonctionnalités.

1.2.2. Environnement de bureau

Kali Linux supporte divers environnements de bureau pour offrir aux utilisateurs la flexibilité de choisir l'interface qui correspond le mieux à leurs besoins et préférences. Voici quelques-uns des environnements de bureau les plus populaires disponibles sur **Kali Linux** :

- **GNOME** : C'est l'environnement de bureau par défaut de **Kali Linux**. **GNOME** est connu pour son interface utilisateur simple et épurée. Il est idéal pour ceux qui recherchent une expérience utilisateur moderne et intuitive. **GNOME** est hautement personnalisable avec une vaste gamme d'extensions disponibles, permettant aux utilisateurs de modifier l'apparence et la fonctionnalité de leur bureau selon leurs besoins spécifiques.
- **KDE Plasma** : Connu pour sa puissante personnalisation, **KDE Plasma** est un choix populaire pour les utilisateurs qui souhaitent une interface hautement configurable. Avec ses nombreuses options de widgets, de thèmes et de configurations, **KDE** permet aux utilisateurs de créer un environnement de travail qui s'adapte parfaitement à leurs préférences de workflow. Il est particulièrement apprécié des utilisateurs avancés qui ont besoin de contrôler finement leur espace de travail.
- **Xfce** : est un environnement de bureau léger, ce qui le rend idéal pour les systèmes avec des ressources limitées ou pour les utilisateurs qui préfèrent une approche minimaliste. Malgré sa simplicité, **Xfce** reste très personnalisable et suffisamment flexible pour être ajusté aux besoins spécifiques de sécurité et de performance.

1.2.3. Métapaquets

Kali Linux offre une fonctionnalité très utile pour ses utilisateurs sous forme de **métapaquets**, qui simplifient grandement l'installation groupée d'outils de sécurité. Ces métapaquets sont conçus pour regrouper et installer des ensembles d'outils relatifs à des besoins spécifiques en matière de cybersécurité, ce qui permet une configuration plus rapide et plus ciblée des environnements de travail.

1.2.4. Qu’est-ce qu’un métapaquets

Un **métapaquet** ne contient pas d'outils en lui-même, il s'agit plutôt d'une collection de dépendances vers d'autres paquets. Lorsqu'un utilisateur installe **un métapaquet**, il installe automatiquement tous les paquets auxquels il fait référence. Cela est particulièrement utile dans **Kali Linux**, où les utilisateurs peuvent avoir besoin de différents ensembles d'outils pour différents types de tests de pénétration ou de tâches de sécurité.

1.2.5. Exemples de Métapaquets dans Kali Linux

Kali Linux inclut plusieurs **métapaquets**, chacun étant conçu pour un type spécifique d'analyse ou de test de sécurité :

- **Kali-linux-full** : Ce métapaquet installe tous les outils disponibles dans **Kali Linux**, offrant une suite complète pour ceux qui ont besoin de toutes les fonctionnalités possibles.
- **Kali-linux-top10** : Il regroupe les dix outils les plus populaires et les plus utilisés dans **Kali Linux**, idéal pour ceux qui commencent avec les tests de pénétration.
- **Kali-linux-forensic** : Ce paquet est destiné aux professionnels de la cyber forensique. Il contient des outils spécifiques pour l'analyse forensique, aidant les utilisateurs à examiner les systèmes après un incident de sécurité.
- **Kali-linux-wireless** : Ce métapaquet est parfait pour ceux qui se spécialisent dans les tests de sécurité des réseaux sans fil, regroupant des outils comme **Aircrack-ng** et **Reaver.**

1.3. Scénarios d’utilisation

Kali Linux est conçu pour être utilisé dans des scénarios de tests de pénétration légaux et éthiques, où les professionnels de la sécurité évaluent les systèmes de sécurité d'une organisation de manière contrôlée pour découvrir et corriger les vulnérabilités avant qu'un attaquant malveillant ne puisse les exploiter.

1.3.1. Test de pénétration

Dans un test de pénétration de réseau, les professionnels utilisent **Kali** pour scanner les systèmes pour identifier les ports ouverts et les services en exécution. Des outils comme **Nmap** permettent de réaliser des scans de ports pour découvrir des points d'entrée non sécurisés. Une fois les ports et services identifiés, des outils comme **Metasploit** peuvent être utilisés pour exploiter les vulnérabilités connues dans ces services, permettant aux testeurs de simuler des attaques pour évaluer la résilience du réseau.

1.3.2. Test de sécurité des applications web

Pour les applications web, des outils comme **Burp Suite** ou **OWASP ZAP** sont fréquemment utilisés pour tester la sécurité des interfaces web. Ces outils peuvent automatiser le processus de test pour identifier des failles de sécurité courantes comme les **injections SQL**, le **cross-site scripting (XSS)**, et le **cross-site request forgery (CSRF).** Les résultats aident à comprendre comment un attaquant pourrait exploiter ces vulnérabilités dans un environnement réel.

1.3.3. Audits de sécurité Wi-Fi

Kali Linux est également équipé d'outils spécialement conçus pour tester la sécurité des réseaux sans fil. **Aircrack-ng** est un ensemble d'outils permettant de tester la sécurité des réseaux Wi-Fi en tentant de craquer les mots de passe **WEP** et **WPA2** à travers des attaques comme le cracking de clés et d'autres techniques de récupération de clés. Cela permet aux professionnels de vérifier la force des mots de passe et la configuration de sécurité du réseau Wi-Fi.

1.3.4. Évaluation de la sécurité physique

Kali inclut des outils qui peuvent être utilisés pour tester la sécurité physique des infrastructures. Par exemple, des outils comme **USB Rubber Ducky** peuvent être utilisés pour simuler des attaques via des dispositifs USB malveillants qui exécutent automatiquement des commandes lorsqu'ils sont connectés à un système. Cela peut démontrer la vulnérabilité à des attaques physiques et inciter à améliorer les politiques de sécurité liées aux dispositifs physiques.

1.3.5. Tests de réponse à incident et forensique

Kali contient également des outils de forensique numérique comme **Autopsy** et **Foremost**, qui peuvent être utilisés pour récupérer des données après une attaque simulée. Ces outils permettent aux testeurs de comprendre quelles données pourraient être récupérées par un attaquant après une intrusion et d'évaluer l'efficacité des mesures de réponse à incidents.

1.4. Communauté et Ressources Éducatives

1.4.1. Rôle de la communauté dans le support et le développement de Kali Linux

La communauté joue un rôle crucial dans le développement et le soutien de Kali Linux. Elle est composée de professionnels de la sécurité, de développeurs, d'étudiants et d'enthousiastes qui contribuent de différentes manières :

- **Forums et groupes d'utilisateurs** : Les forums de **Kali Linux**, comme ceux disponibles sur le site officiel, offrent un espace pour que les utilisateurs posent des questions, partagent des connaissances et discutent des problèmes. Ces forums sont essentiels pour le support entre pairs, où les utilisateurs peuvent obtenir de l'aide pour résoudre des problèmes techniques ou pour obtenir des conseils sur l'utilisation des outils.
- **Contributions au code source** : **Kali Linux** est un projet open source, ce qui permet à quiconque de contribuer à son développement. Les utilisateurs peuvent soumettre des corrections de bugs, proposer de nouvelles fonctionnalités ou améliorer les outils existants via des plateformes comme **GitHub**.
- **Retours et tests** : Les membres de la communauté aident également en testant les nouvelles versions de logiciels et en signalant des bugs ou des problèmes de sécurité, ce qui aide à maintenir la stabilité et la sécurité de la distribution.

1.4.2. Ressources éducatives pour apprendre à utiliser Kali Linux

Pour ceux qui souhaitent apprendre à utiliser **Kali Linux**, plusieurs ressources sont disponibles :

- **Cours en ligne** : Il existe de nombreux cours en ligne gratuits et payants qui enseignent comment utiliser Kali Linux pour les tests de pénétration. Des plateformes comme **Udemy, Coursera** et **Cybrary** offrent des cours spécifiques sur **Kali** et ses outils.
- **Certifications** : **Offensive Security**, la société derrière **Kali Linux**, offre plusieurs certifications très respectées dans l'industrie de la sécurité, notamment **l'Offensive Security Certified Professional (OSCP).**
- **Ateliers et conférences** : Des événements comme des ateliers, des conférences et des meetups offrent souvent des sessions pratiques et des démonstrations en direct.

2. Distribution Parrot OS

2.1. Introduction

Parrot OS est une distribution Linux axée sur la sécurité, souvent comparée à **Kali Linux** pour ses fonctionnalités et ses objectifs similaires. Cependant, **Parrot OS** se distingue par quelques caractéristiques et un positionnement unique qui le rendent intéressant pour une gamme spécifique d'utilisateurs.

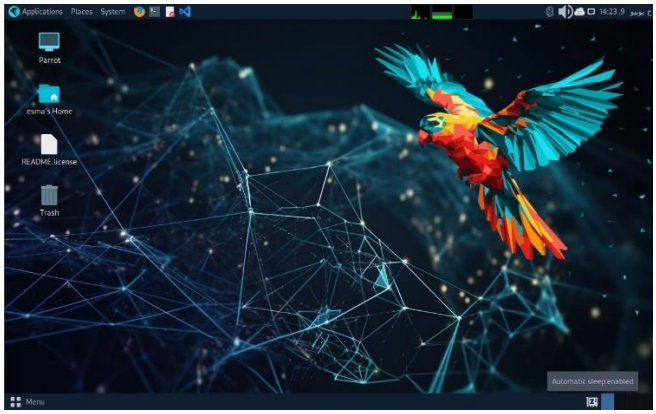

***Figure 2 : Parrot OS** Distribution*

2.1.1. Caractéristiques Uniques de Parrot OS

- **Sécurité et confidentialité** : **Parrot OS** est conçu avec un fort accent sur la sécurité et la confidentialité. En plus des outils de test de pénétration, il inclut des programmes destinés à préserver la confidentialité de l'utilisateur, comme **Tor, Anonsurf** (qui anonymise le trafic internet), et d'autres outils de cryptographie.
- **Légèreté** : Contrairement à d'autres distributions, **Parrot OS** est particulièrement léger. Il est optimisé pour fonctionner efficacement sur des ordinateurs avec des ressources limitées, ce qui le rend accessible à un plus large éventail d'utilisateurs, y compris ceux qui disposent de matériel moins puissant.
- **Environnement de bureau** : **Parrot OS** utilise **MATE** comme environnement de bureau par défaut, une dérivation de **GNOME 2**, connue pour sa simplicité et sa fonctionnalité.

Cela offre une expérience utilisateur fluide et conviviale, surtout pour ceux qui préfèrent une interface classique.

- **Polyvalence** : En plus des outils de cybersécurité, **Parrot OS** est équipé pour des utilisations en programmation, développement, et même pour les tâches quotidiennes. Cette polyvalence le rend utile non seulement pour les professionnels de la sécurité mais aussi pour les développeurs et les utilisateurs généraux.

2.1.2. Positionnement par Rapport à Kali Linux

Bien que **Parrot OS** et **Kali Linux** partagent de nombreux outils de sécurité similaires, **Parrot OS** se positionne comme étant plus polyvalent. Alors que **Kali** est presque exclusivement centré sur les tests de pénétration, **Parrot OS** offre un éventail plus large d'outils qui peuvent également servir à d'autres fins informatiques, faisant de lui une distribution plus généraliste avec un fort accent sur la sécurité et la confidentialité.

2.1.3. Brève Histoire et Origines

Parrot OS a été lancé en 2013 par **Lorenzo "Palinuro" Faletra** et l'équipe de **Frozenbox**. Le système a été conçu pour fournir une plateforme qui non seulement intègre des outils de sécurité, mais qui soit aussi orientée vers la confidentialité, l'anonymat et la cryptographie. L'idée était de créer une distribution qui soit à la fois utile pour les professionnels de la sécurité et pratique pour un usage quotidien avec un accent sur la protection de la vie privée.

2.1.4. Objectifs Initiaux

Les objectifs initiaux de **Parrot OS** étaient de développer une distribution Linux qui puisse être utilisée tant pour les tests de sécurité que pour les activités quotidiennes tout en maintenant l'utilisateur anonyme et sécurisé en ligne. Cela a été réalisé en incorporant des outils de sécurité robustes et des fonctionnalités de confidentialité, ainsi qu'en assurant que le système puisse être utilisé pour le développement et d'autres tâches informatiques générales.

2.2. Architecture de Parrot OS

2.2.1. Importance de Debian comme Base pour Parrot OS

L'utilisation de Debian comme base pour **Parrot OS** offre plusieurs avantages cruciaux, notamment en termes de stabilité et de sécurité :

- **Stabilité éprouvée** : Debian est reconnue pour sa stabilité et sa fiabilité, ce qui est essentiel pour une distribution orientée sécurité comme **Parrot OS**. En utilisant Debian, **Parrot OS** bénéficie d'une fondation solide sur laquelle les utilisateurs peuvent compter pour des opérations de sécurité critiques et des applications du quotidien.

- **Sécurité renforcée** : Debian dispose d'une solide réputation en matière de sécurité, avec des mises à jour régulières qui adressent les vulnérabilités connues et améliorent la sécurité globale du système. Pour **Parrot OS**, cela signifie avoir une base sécurisée qui est constamment revue et renforcée contre les menaces émergentes.

- **Cycle de vie supporté à long terme** : Debian offre un support à long terme pour chaque version, garantissant ainsi que les systèmes basés sur Debian, comme **Parrot OS**, bénéficient de correctifs et de mises à jour pendant une période prolongée. Cela est crucial pour maintenir l'intégrité et la sécurité du système au fil du temps.

2.2.2. Avantages de l'Utilisation de MATE

MATE, l'environnement de bureau utilisé par **Parrot OS,** est une dérivation de **GNOME 2**, connu pour sa légèreté et son efficacité. Voici les avantages clés de l'utilisation de MATE dans **Parrot OS :**

- **Performance améliorée** : **MATE** est conçu pour être léger, ce qui le rend idéal pour les systèmes avec des ressources limitées et pour les utilisateurs qui préfèrent une expérience rapide et réactive. Cela permet à **Parrot OS** de fonctionner efficacement même sur des machines moins puissantes.
- **Simplicité et accessibilité** : L'interface de **MATE** est simple et intuitive, ce qui la rend accessible aux utilisateurs de tous niveaux. Cette accessibilité est particulièrement bénéfique pour les utilisateurs qui sont nouveaux dans le monde des distributions Linux basées sur la sécurité.
- **Personnalisation** : **MATE** offre des niveaux élevés de personnalisation, permettant aux utilisateurs de **Parrot OS** de modifier l'apparence et le comportement du système selon leurs préférences ou besoins spécifiques. Cette flexibilité est importante pour les professionnels de la sécurité qui peuvent avoir besoin de configurer leur environnement de travail de manière très spécifique.
- **Compatibilité** : Étant une continuation de **GNOME 2, MATE** est compatible avec une large gamme d'applications conçues pour **GNOME**, garantissant que les utilisateurs de **Parrot OS** ont accès à une vaste bibliothèque de logiciels.

2.3. Caractéristiques Clés et Innovations

Parrot OS intègre une série d'outils et de services spécialement conçus pour le cryptage, la confidentialité en ligne et la protection contre les surveillances. Ces fonctionnalités renforcent sa position comme une distribution Linux de choix pour les utilisateurs qui accordent une grande importance à la sécurité et à la confidentialité.

2.3.1. Outils pour le Cryptage et la Confidentialité

- **Cryptage de disque complet** : **Parrot OS** offre des options pour le cryptage de disque complet, utilisant des technologies comme **LUKS** (Linux Unified Key Setup) pour chiffrer les données stockées sur les disques durs. Ceci est crucial pour protéger les données au repos contre les accès non autorisés.
- **GnuPG** : Ce logiciel intégré permet le chiffrement et la signature de données. **GnuPG** est essentiel pour la sécurisation des communications et des fichiers, permettant aux utilisateurs d'échanger des informations de manière sécurisée.
- **Cryptage de réseau** : **Parrot OS** inclut divers outils pour sécuriser les communications réseau, comme **OpenVPN**, qui permet de créer des réseaux privés virtuels sécurisés, et **WireGuard**, une solution **VPN** plus récente et performante.

2.3.2. Anonymat et Protection Contre la Surveillance

Anonsurf est un outil phare de **Parrot OS** pour l'anonymat en ligne. Il reroute tout le trafic internet à travers le réseau **Tor**, masquant ainsi l'adresse **IP** de l'utilisateur et cryptant le trafic pour protéger contre l'interception et la surveillance. Ceci est particulièrement utile pour les

utilisateurs dans des régions où la surveillance en ligne est intensive ou pour ceux qui veulent éviter d'être tracés lors de leurs activités sur internet.

En plus d'**Anonsurf**, **Parrot OS** inclut des outils comme **I2P**, un réseau anonyme qui offre des fonctionnalités similaires à **Tor** mais se concentre sur l'accès interne au réseau, et **Tor Browser**, un navigateur web optimisé pour l'utilisation du réseau **Tor**.

2.3.3. Support pour une Variété de Matériel et Configurations

Parrot OS est également conçu pour être hautement compatible avec une large gamme de matériel et de configurations, y compris :

- **Ordinateurs classiques** : **Parrot OS** peut être installé sur la majorité des ordinateurs personnels, y compris les configurations plus anciennes ou moins puissantes grâce à son environnement de bureau léger.
- **IoT et systèmes embarqués** : Avec la montée de l'Internet des Objets **(IoT),** la sécurité de ces dispositifs est devenue primordiale. **Parrot OS** propose des versions spécifiques qui peuvent être utilisées pour sécuriser ces appareils, offrant des outils pour tester la sécurité des systèmes embarqués et IoT.
- **Machines virtuelles et serveurs** : **Parrot OS** peut être exécuté dans des environnements virtuels ou déployé sur des serveurs, offrant une plateforme sécurisée pour les tests de pénétration et la surveillance de la sécurité en environnements contrôlés.

2.4. Communauté et Support

Le développement de **Parrot OS,** tout comme beaucoup d'autres distributions Linux, repose fortement sur sa communauté active. Cette communauté ne se limite pas seulement aux développeurs, mais s'étend aussi aux utilisateurs, aux professionnels de la sécurité, aux éducateurs, et aux passionnés de technologie. Voici quelques aspects clés du rôle de la communauté dans le développement de **Parrot OS** :

2.4.1. Développement Collaboratif

- **Contribution au Code Source** : **Parrot OS** étant un projet open-source, il bénéficie des contributions de développeurs du monde entier. Les membres de la communauté peuvent soumettre des patches, des fonctionnalités nouvelles ou améliorées, et des corrections de bugs via des plateformes comme **GitHub**.
- **Développement d'Outils :** De nombreux outils intégrés dans **Parrot OS** sont également développés par la communauté. Cela permet non seulement de maintenir les outils à jour avec les dernières tendances en matière de sécurité informatique mais aussi d'innover en introduisant de nouvelles solutions aux problèmes émergents.
- **Tests et Retours d'Utilisateurs :** Les membres de la communauté jouent un rôle crucial dans le test des nouvelles versions de **Parrot OS,** fournissant des retours essentiels qui aident à peaufiner la distribution avant sa sortie officielle.

2.4.2. Ressources pour Utilisateurs Novices et Experts

Parrot OS s'efforce de fournir une large gamme de ressources pour tous ses utilisateurs, qu'ils soient débutants ou experts en sécurité informatique :

- **Documentation** : **Parrot OS** dispose d'une documentation complète qui couvre tout, des bases de l'installation aux instructions avancées pour l'utilisation des outils de sécurité. Cette documentation est régulièrement mise à jour pour refléter les dernières versions et fonctionnalités.
- **Forums de la Communauté** : Les forums de **Parrot OS** sont un lieu vital pour le support et l'échange de connaissances. Les utilisateurs peuvent y poser des questions, partager des expériences, et obtenir des conseils sur des problèmes spécifiques.
- **Cours et Webinaires** : Des cours en ligne et des webinaires sont parfois organisés par des membres de la communauté ou des experts en sécurité, offrant des sessions d'apprentissage structurées pour ceux qui cherchent à approfondir leur connaissance de **Parrot OS** et de ses applications en cybersécurité.

3. Comparaison entre Kali Linux et Parrot OS

3.1. Points Communs

3.1.1. Base Debian

Tant **Parrot OS** que **Kali Linux** sont basés sur **Debian**, ce qui leur confère une fondation solide en termes de stabilité, de sécurité et de support. La base Debian garantit également une compatibilité étendue avec une vaste gamme de matériel et de logiciels, facilitant l'intégration et la gestion des systèmes. En étant basées sur Debian, ces distributions bénéficient des mises à jour régulières et d'une communauté de développeurs active, ce qui assure un maintien constant de la sécurité et de la stabilité du système.

3.1.2. Outils de sécurité

Les deux distributions incluent une collection exhaustive d'outils dédiés aux tests de pénétration, à l'audit de sécurité, à la criminalistique numérique, et à d'autres activités liées à la sécurité informatique. Cela les rend idéales pour les professionnels de la sécurité et les chercheurs en cybersécurité. **Parrot OS** et **Kali Linux** intègrent des outils comme **Nmap, Metasploit, Wireshark, John the Ripper**, et bien d'autres, permettant une analyse complète des systèmes et réseaux pour identifier et exploiter les vulnérabilités. Cette richesse d'outils préinstallés permet aux utilisateurs de démarrer immédiatement des activités de sécurité sans nécessiter de configuration supplémentaire.

3.2. Points de différence

3.2.1. Orientation vers la Confidentialité et l'Anonymat

- **Parrot OS :**
    - Met un accent particulier sur l'anonymat et la confidentialité en intégrant des outils comme **Anonsurf**, qui reroute le trafic internet à travers **Tor**. Cette fonctionnalité est particulièrement utile pour masquer l'identité et la localisation

de l'utilisateur, rendant **Parrot OS** une option privilégiée pour ceux qui priorisent la confidentialité au-delà des simples fonctionnalités de sécurité. De plus, **Parrot OS** inclut d'autres outils de protection de la vie privée comme les gestionnaires de mots de passe, les chiffreurs de fichiers, et les outils de suppression sécurisée de données.

- **Kali Linux :**
    - Bien que **Kali** inclue des outils permettant de sécuriser les communications, son focus principal reste les tests de pénétration et l'audit de sécurité sans un aussi grand accent sur l'anonymat. **Kali** est principalement conçu pour les professionnels de la sécurité informatique nécessitant des outils puissants pour les tests de pénétration. Néanmoins, les utilisateurs peuvent ajouter des outils de confidentialité à Kali, mais cela nécessite des configurations supplémentaires.

3.2.2. Environnement de Bureau

- **Parrot OS :**
    - Utilise **MATE,** un environnement de bureau léger, ce qui rend la distribution plus accessible pour les machines avec des ressources systèmes limitées. **MATE** est également reconnu pour son interface utilisateur traditionnelle et efficace, offrant une expérience utilisateur fluide même sur du matériel ancien ou peu performant. L'accent sur la légèreté et la performance fait de **Parrot OS** un choix approprié pour les utilisateurs recherchant une interface simple mais fonctionnelle.
- **Kali Linux :**
    - Offre une flexibilité plus grande dans le choix de l'environnement de bureau, avec des options comme **GNOME, KDE**, et **XFCE**, satisfaisant ainsi une gamme plus large de préférences utilisateurs. Cette flexibilité permet aux utilisateurs de personnaliser leur environnement de travail en fonction de leurs besoins spécifiques et de leur matériel. Par exemple, **GNOME** offre une interface moderne et riche en fonctionnalités, tandis que **XFCE** est conçu pour être léger et économe en ressources.

3.2.3. Public Cible

- **Parrot OS :**
    - Cible non seulement les professionnels de la sécurité mais aussi les utilisateurs préoccupés par la surveillance et la vie privée. Cela comprend les journalistes, les activistes, et toute personne soucieuse de protéger son identité en ligne. **Parrot OS** est conçu pour être une plateforme polyvalente, intégrant des outils de sécurité et de confidentialité pour répondre aux besoins d'un public diversifié. La distribution inclut également des fonctionnalités éducatives pour les débutants en cybersécurité, rendant l'apprentissage accessible à tous.

- **Kali Linux :**
    - Principalement orienté vers les professionnels de la sécurité informatique et les auditeurs, offrant des outils et des ressources spécifiquement conçus pour le pentesting professionnel et l'éducation en cybersécurité. **Kali** est réputé pour sa robustesse et sa pertinence dans les environnements professionnels où des tests de sécurité approfondis sont requis. La distribution est fréquemment mise à jour avec les dernières techniques d'exploitation et de sécurité, assurant aux utilisateurs un accès aux outils les plus récents et les plus efficaces.

Chapitre 2 : Outils de sécurité dans Kali Linux et Parrot OS

1. Outils de sécurité dans Kali Linux

1.1. Vue d'ensemble des catégories d'outils intégrés

- **Analyse de vulnérabilité et audit de sécurité :** Cette catégorie d'outils est essentielle pour identifier les failles de sécurité potentielles dans les systèmes cibles. En examinant minutieusement les logiciels, les configurations et les paramètres, ces outils peuvent mettre en évidence les points faibles qui pourraient être exploités par des attaquants. De plus, ils permettent souvent de générer des rapports détaillés sur les vulnérabilités détectées, facilitant ainsi la prise de mesures correctives appropriées pour renforcer la sécurité des systèmes.

- **Test de pénétration :** Les outils de test de pénétration sont conçus pour simuler des attaques informatiques afin d'évaluer la résilience d'un système face à des menaces potentielles. En reproduisant les techniques et les méthodes utilisées par les attaquants, ces outils permettent aux professionnels de la sécurité de tester la robustesse des défenses d'un système. Cela peut inclure des tests d'intrusion sur les réseaux, les applications web, les applications mobiles et d'autres composants de l'infrastructure informatique.

- **Forensics & Reverse Engineering :** Cette catégorie d'outils est indispensable pour les enquêtes post-incident, la récupération de données et l'analyse des incidents de sécurité. Les outils de forensics permettent aux experts en sécurité de collecter des preuves numériques, d'analyser les journaux d'activité et de reconstruire les événements survenus lors d'incidents de sécurité. Parallèlement, les outils de reverse engineering sont utilisés pour examiner le fonctionnement interne des logiciels et matériels, en permettant de comprendre leur fonctionnement, de détecter les failles de sécurité et de développer des contre-mesures appropriées.

- **Surveillance et analyse du réseau :** Ces outils sont essentiels pour surveiller et analyser le trafic réseau, détecter les comportements suspects et répondre aux menaces en temps réel. En capturant et en analysant les paquets de données qui transitent sur le réseau, ces outils permettent aux administrateurs de détecter les tentatives d'intrusion, les attaques par déni de service et d'autres activités malveillantes. De plus, ils offrent souvent des fonctionnalités avancées telles que la corrélation d'événements, la visualisation du trafic et la génération d'alertes en cas d'anomalies.

- **Exploitation d'applications :** Cette catégorie d'outils est utilisée pour tester les applications et services web afin de détecter et d'exploiter les vulnérabilités qui pourraient être exploitées par des attaquants. En utilisant des techniques telles que

l'injection de code, la manipulation des paramètres d'URL et les attaques par force brute, ces outils permettent aux testeurs de sécurité d'identifier les failles de sécurité telles que les injections **SQL**, les **XSS** (Cross-Site Scripting) et les failles d'authentification.

- **Anonymat et vie privée :** Ces outils sont conçus pour permettre aux utilisateurs de protéger leur vie privée en ligne et de masquer leur identité sur Internet. En utilisant des techniques telles que le chiffrement, les réseaux privés virtuels **(VPN)** et les réseaux anonymes comme **Tor**, ces outils permettent aux utilisateurs de naviguer sur le web de manière anonyme et sécurisée, en évitant la surveillance et la censure. De plus, ils offrent souvent des fonctionnalités supplémentaires telles que la navigation sans suivi, le blocage des publicités et la protection contre le pistage en ligne.

1.2. Analyse détaillée par catégorie

1.2.1. Analyse de vulnérabilité et audit de sécurité

- **Nmap :** Cet outil, connu sous le nom de **"Network Mapper",** est un scanner de ports réseau largement utilisé par les professionnels de la sécurité informatique pour découvrir des hôtes et des services sur un réseau. Il permet d'identifier les systèmes actifs, de cartographier le réseau et de détecter les ports ouverts, offrant ainsi une vue d'ensemble de la surface d'attaque potentielle d'un réseau.
- **OpenVAS :** L'Open Vulnerability Assessment System **(OpenVAS)** est un outil d'analyse de vulnérabilité open source qui effectue des tests automatisés pour détecter les vulnérabilités dans les systèmes cibles. En utilisant une base de données constamment mise à jour des vulnérabilités connues, **OpenVAS** peut identifier les failles de sécurité potentielles dans les logiciels, les configurations système et les services réseau, aidant ainsi les organisations à renforcer leur posture de sécurité.

1.2.2. Test de pénétration

- **Metasploit Framework :** Le **Metasploit Framework** est un outil puissant de test de pénétration et d'exploitation largement utilisé par les professionnels de la sécurité pour développer, tester et exécuter des exploits contre des cibles vulnérables. En fournissant une bibliothèque d'exploits pré-construits, des payloads et des modules auxiliaires, **Metasploit** simplifie le processus de développement et d'exécution d'attaques, permettant aux chercheurs en sécurité de tester la résilience des systèmes face aux attaques.
- **Hydra :** est un outil de craquage de mots de passe polyvalent qui prend en charge de nombreux protocoles de connexion, y compris **SSH, FTP, HTTP**, et bien d'autres. En utilisant des attaques par force brute ou par dictionnaire, Hydra tente de deviner les identifiants d'accès en testant différentes combinaisons de mots de passe, permettant ainsi aux professionnels de la sécurité de tester la robustesse des mécanismes d'authentification d'un système.

1.2.3. Forensics & Reverse Engineering

- **Autopsy :** est une interface graphique conviviale pour la forensique numérique, utilisée par les enquêteurs pour analyser les images disque et les données provenant de dispositifs de stockage numérique. En permettant l'extraction et l'analyse des données, la récupération des fichiers supprimés et la visualisation des informations pertinentes,

Autopsy aide les enquêteurs à reconstruire les événements survenus lors d'incidents de sécurité et à collecter des preuves numériques utilisables.

- **Radare2 :** est un framework de reverse engineering avancé utilisé pour l'analyse binaire et la **rétro-ingénierie** de logiciels. En fournissant des outils puissants pour désassembler, décompiler, analyser et manipuler des binaires, **Radare2** permet aux chercheurs en sécurité et aux analystes de comprendre le fonctionnement interne des logiciels, d'identifier les vulnérabilités et de développer des contre-mesures appropriées pour renforcer la sécurité des systèmes.

1.2.4. Surveillance et analyse du réseau

- **Wireshark :** est un analyseur de protocole réseau puissant qui permet aux administrateurs système et aux professionnels de la sécurité de capturer et d'inspecter le trafic réseau en profondeur. En affichant les paquets de données échangés entre les hôtes sur un réseau, **Wireshark** permet d'identifier les comportements suspects, les attaques en cours et les problèmes de performance du réseau, facilitant ainsi la détection et la résolution des problèmes de sécurité.
- **Snort :** est un système de détection d'intrusion en temps réel **(IDS)** et de prévention d'intrusion **(IPS)** largement utilisé pour surveiller le trafic réseau et détecter les activités malveillantes. En utilisant des règles de détection personnalisables, **Snort** peut identifier les tentatives d'exploitation, les scans de ports suspects et d'autres comportements anormaux, déclenchant des alertes en temps réel pour informer les administrateurs de la sécurité des menaces éventuelles.

1.2.5. Exploitation d'applications

- **Burp Suite :** est un ensemble d'outils complet conçu pour tester la sécurité des applications web. En fournissant des fonctionnalités telles que le scan de vulnérabilités, l'interception de requêtes **HTTP**, l'injection de payloads et la manipulation des cookies, **Burp Suite** permet aux testeurs de sécurité de découvrir et d'exploiter les failles de sécurité telles que les injections **SQL**, les **XSS** et les failles d'authentification.
- **SQLMap :** est un outil automatisé spécialement conçu pour l'injection **SQL** et l'exploitation de bases de données. En détectant et en exploitant les vulnérabilités d'injection **SQL** dans les applications web, **SQLMap** permet aux chercheurs en sécurité de récupérer des données sensibles, d'exécuter des commandes sur le serveur de base de données et de compromettre le système hôte, mettant ainsi en évidence les risques potentiels pour la sécurité des données.

1.2.6. Anonymat et vie privée

- **Tor :** est un réseau décentralisé conçu pour anonymiser le trafic Internet en routant les communications à travers une série de nœuds de relais. En cryptant le trafic et en masquant l'adresse **IP** de l'utilisateur, **Tor** permet aux utilisateurs de naviguer sur le web de manière anonyme, en évitant la surveillance gouvernementale, la censure en ligne et le suivi des activités en ligne par les annonceurs et les fournisseurs de services Internet.
- **Proxychains :** est un outil de routage de trafic qui permet de chaîner des proxys et de router le trafic à travers plusieurs serveurs proxy pour masquer l'origine de la connexion. En utilisant des proxys anonymes et des réseaux privés virtuels **(VPN)**, **Proxychains** offre une couche supplémentaire de confidentialité et de sécurité en ligne, permettant aux

utilisateurs de naviguer sur le web de manière anonyme et de contourner les restrictions géographiques et les blocages de contenu.

1.3. Evaluation des fonctionnalités et performances

L'évaluation des fonctionnalités et des performances de ces outils dépend de nombreux facteurs, notamment de la complexité des scénarios de test, de la configuration système, de la documentation disponible et de la communauté de support. Certains outils sont plus adaptés à certaines tâches que d'autres, et il est souvent nécessaire d'expérimenter plusieurs outils pour trouver celui qui convient le mieux à une situation donnée.

De plus, la mise à jour régulière des outils est essentielle pour garantir qu'ils restent efficaces contre les nouvelles menaces et vulnérabilités. La communauté open source derrière Kali Linux travaille continuellement à améliorer et à mettre à jour les outils inclus dans la distribution, ce qui contribue à maintenir sa réputation en tant que choix populaire pour les professionnels de la sécurité et les chercheurs en sécurité informatique.

2. Outils de sécurité dans Parrot OS

2.1. Vue d'ensemble des outils intégrés

Parrot OS est hautement réputé dans le domaine de la sécurité informatique en raison de sa remarquable panoplie d'outils intégrés, minutieusement sélectionnés pour répondre aux besoins les plus diversifiés des professionnels de la cybersécurité, des chercheurs en sécurité, ainsi que des adeptes du hacking éthique. Explorez en détail les différentes catégories d'outils qui enrichissent l'écosystème de **Parrot OS** :

- **Tests d'intrusion et de pénétration :** Ces outils sont essentiels pour évaluer la résilience des systèmes informatiques face aux attaques cybernétiques en simulant divers scénarios d'attaques. Ils englobent des fonctionnalités avancées telles que le scanning de ports, la détection de vulnérabilités, l'exploitation des failles, ainsi que les étapes de post-exploitation, fournissant ainsi une approche exhaustive pour tester et renforcer la sécurité des infrastructures.
- **Analyse de vulnérabilités :** Cette catégorie d'outils est cruciale pour identifier et évaluer les failles potentielles dans les systèmes informatiques et les réseaux. Grâce à des techniques sophistiquées de détection, ces outils permettent de repérer les points faibles et de recommander des correctifs appropriés pour renforcer la sécurité des environnements numériques.
- **Surveillance réseau :** Offrant une visibilité en temps réel sur le trafic réseau, ces outils permettent une analyse approfondie des paquets de données échangés, facilitant ainsi la détection proactive des activités suspectes ou malveillantes. Cette surveillance continue contribue à renforcer la posture de sécurité en identifiant rapidement les anomalies et les comportements inhabituels.
- **Protection de la vie privée et anonymat :** Dans un monde numérique où la confidentialité est devenue une préoccupation majeure, cette catégorie d'outils offre des solutions complètes pour préserver la vie privée en ligne. En fournissant des mécanismes d'anonymisation de la navigation sur Internet et en contournant les restrictions de censure en ligne, ces outils offrent aux utilisateurs un contrôle accru sur leur vie numérique.

- **Cryptographie :** Les outils de cryptographie intégrés à **Parrot OS** offrent une gamme complète de fonctionnalités pour sécuriser les données sensibles. Du chiffrement des communications au stockage sécurisé des informations, en passant par la génération de clés cryptographiques et la vérification de l'intégrité des données, ces outils garantissent une protection robuste contre les menaces potentielles.
- **Récupération de données :** En cas de perte accidentelle ou de suppression de données, ces outils spécialisés sont indispensables pour récupérer efficacement les informations cruciales à partir de divers supports de stockage tels que les disques durs, les clés USB et les cartes mémoire. Leur capacité à restaurer les données perdues avec précision et fiabilité en fait des alliés précieux dans les situations d'urgence.

2.2. Analyse détaillée par catégorie

2.2.1. Tests d'intrusion et de pénétration

Parrot OS se dote d'une pléthore d'outils de pointe dédiés aux tests d'intrusion et à la pénétration, assurant ainsi une évaluation approfondie de la sécurité des systèmes. Parmi ces outils, on retrouve :

- **Nmap :** Réputé pour sa polyvalence, **Nmap** est un outil incontournable pour la découverte des dispositifs réseau et le mapping des infrastructures, offrant une visibilité précise sur les configurations réseau.
- **Metasploit :** Cette plateforme renommée est une ressource indispensable pour le développement, les tests et l'exploitation des vulnérabilités. Elle permet aux professionnels de la sécurité de simuler des attaques réelles et d'identifier les failles de sécurité.
- **Aircrack-ng :** Spécialisé dans l'audit des réseaux sans fil, **Aircrack-ng** propose une gamme d'outils puissants pour la détection des vulnérabilités et la sécurisation des réseaux Wi-Fi.

2.2.2. Analyse de vulnérabilités

La catégorie de l'analyse de vulnérabilités regorge d'outils sophistiqués permettant de détecter et de corriger les failles de sécurité. Parmi les plus remarquables, on trouve :

- **OpenVAS :** Reconnu pour sa robustesse, **OpenVAS** est un scanner de vulnérabilités qui identifie les failles de sécurité dans les systèmes et les applications, offrant ainsi une vue détaillée de la posture de sécurité.
- **Nessus :** Avec sa capacité à effectuer une évaluation approfondie de la sécurité, Nessus est un autre scanner de vulnérabilités populaire, offrant des rapports détaillés sur les vulnérabilités détectées et les recommandations de correctifs.

2.2.3. Surveillance réseau

Parrot OS intègre une série d'outils de surveillance réseau permettant une analyse en temps réel du trafic et une détection proactive des activités suspectes. Parmi ces outils, on distingue :

- **Wireshark :** Réputé pour sa convivialité, **Wireshark** est un outil puissant d'analyse de paquets réseau, offrant une visibilité détaillée sur le trafic et les communications réseau.

- **tcpdump :** En tant qu'outil en ligne de commande robuste, **tcpdump** permet la capture et l'analyse efficace du trafic réseau, offrant ainsi un contrôle précis sur les activités réseau.

2.2.4. Protection de la vie privée et anonymat

La préservation de la vie privée et l'anonymat en ligne sont des préoccupations majeures, et **Parrot OS** intègre des outils dédiés pour répondre à ces besoins, notamment :

- **Tor :** En tant que réseau décentralisé de relais, **Tor** permet de naviguer sur Internet de manière anonyme en masquant l'adresse **IP** de l'utilisateur, offrant ainsi une protection robuste de la vie privée en ligne.
- **VPN : Parrot OS** intègre plusieurs clients **VPN** pour sécuriser les connexions Internet et préserver la confidentialité des communications, offrant ainsi une couche supplémentaire de protection contre l'espionnage et la surveillance en ligne.

2.2.5. Cryptographie

La catégorie de la cryptographie joue un rôle essentiel dans la protection des données sensibles et **Parrot OS** propose une gamme d'outils de chiffrement avancés, tels que :

- **GnuPG :** Cette implémentation libre du standard **OpenPGP** offre des fonctionnalités complètes de chiffrement et de signature de données, assurant ainsi l'intégrité et la confidentialité des informations.
- **Cryptsetup :** Spécifiquement conçu pour Linux, **Cryptsetup** permet la configuration et la gestion de volumes chiffrés, offrant une protection robuste des données sensibles contre les accès non autorisés.

2.2.6. Récupération de données

En cas de perte accidentelle de données, **Parrot OS** propose une série d'outils de récupération efficaces pour restaurer les informations perdues, notamment :

- **TestDisk :** Réputé pour sa puissance, **TestDisk** est un outil essentiel pour récupérer des partitions perdues et restaurer des fichiers supprimés, offrant ainsi une solution fiable pour la récupération de données.
- **PhotoRec :** Spécialisé dans la récupération de fichiers multimédias, y compris des photos, des vidéos et des documents, **PhotoRec** est un outil polyvalent pour restaurer les données perdues à partir de divers supports de stockage.

2.3. Evaluation des fonctionnalités et performances

- **Richesse fonctionnelle : Parrot OS** se distingue par sa richesse fonctionnelle exceptionnelle, offrant une panoplie complète d'outils de sécurité conçus pour couvrir tous les aspects de la protection numérique. Des tests de pénétration à la préservation de la confidentialité en ligne, en passant par la récupération de données, chaque outil est sélectionné avec soin pour répondre aux besoins diversifiés des utilisateurs. Cette diversité permet aux professionnels de la sécurité informatique, aux chercheurs en sécurité, ainsi qu'aux passionnés de hacking éthique de trouver les ressources nécessaires pour mener à bien leurs missions, quelle que soit leur complexité.
- **Performances : Parrot OS** s’efforce de fournir des performances optimales à ses utilisateurs, même sur des configurations matérielles moins puissantes. La majorité des

outils intégrés sont bien optimisés, garantissant une exécution efficace des tâches de sécurité. Cependant, il est important de noter que les performances peuvent varier en fonction de la charge de travail et de la complexité des opérations. Dans l'ensemble, **Parrot OS** s'engage à offrir une expérience fluide et réactive, même lors de l'exécution de tâches intensives en ressources.

- **Facilité d'utilisation :** La convivialité est au cœur de la conception de **Parrot OS.** La distribution vise à rendre les outils de sécurité accessibles même aux utilisateurs novices, en fournissant une documentation détaillée et des interfaces utilisateur intuitives. Grâce à cette approche, les utilisateurs peuvent facilement naviguer à travers les différentes fonctionnalités et bénéficier pleinement des capacités offertes par les outils intégrés. Cette convivialité renforce l'accessibilité de la plateforme, permettant à un large éventail d'utilisateurs de tirer parti de ses fonctionnalités sans nécessiter une expertise technique avancée.

3. Installation des packages via APT

3.1. Introduction

L'installation de logiciels et de packages est une composante essentielle de tout système d'exploitation. **Parrot OS** et **Kali Linux**, bien que similaires dans leur base **Debian**, présentent des particularités et des optimisations qui répondent aux besoins spécifiques de leurs utilisateurs. Cette section examine en profondeur le processus d'installation des packages via **APT** (Advanced Package Tool), les similitudes et les différences dans l'utilisation de cet outil entre les deux distributions.

3.2. Processus d'installation

3.2.1. Parrot OS

Parrot OS utilise **APT** pour gérer ses paquets logiciels. Voici un aperçu détaillé du processus :

- **Mise à jour des listes de paquets :** La commande ***sudo apt update*** permet de synchroniser les listes de paquets disponibles avec les dépôts configurés. Cela garantit que les informations sur les logiciels disponibles sont à jour.
- **Installation de paquets :** Pour installer un nouveau logiciel, les utilisateurs peuvent utiliser ***sudo apt install [nom_du_paquet]***. **Parrot OS** propose une vaste gamme de paquets dans ses dépôts, incluant des outils de sécurité, des logiciels de productivité, et des outils axés sur la confidentialité.
- **Mise à jour des paquets installés :** La commande ***sudo apt upgrade*** met à jour tous les paquets installés vers leurs versions les plus récentes disponibles dans les dépôts.
- **Suppression de paquets :** Pour désinstaller un logiciel, les utilisateurs peuvent utiliser ***sudo apt remove [nom_du_paquet]***. Cette commande supprime le paquet spécifié tout en conservant les fichiers de configuration.
- **Nettoyage des paquets inutiles :** ***sudo apt autoremove*** supprime les paquets qui ont été installés en tant que dépendances mais qui ne sont plus nécessaires.

Parrot OS inclut également des dépôts spécifiques qui contiennent des logiciels axés sur la confidentialité et l'anonymat, comme **Anonsurf**, ainsi que des outils de sécurité avancés.

3.2.2. Kali Linux

Kali Linux utilise également APT pour la gestion des paquets, avec quelques optimisations pour répondre aux besoins des professionnels de la sécurité :

- **Mise à jour des listes de paquets :** La commande ***sudo apt update*** est utilisée de la même manière pour synchroniser les listes de paquets disponibles avec les dépôts de Kali.
- **Installation de paquets :** ***sudo apt install [nom_du_paquet]*** permet d'installer des logiciels spécifiques. **Kali Linux** propose une vaste gamme d'outils de sécurité dans ses dépôts, souvent les versions les plus récentes et les plus performantes.
- **Mise à jour des paquets installés :** ***sudo apt upgrade*** met à jour les paquets installés. **Kali** inclut également des commandes supplémentaires comme ***sudo apt full-upgrade*** qui effectue une mise à niveau complète du système, incluant les modifications de dépendances.
- **Suppression de paquets :** ***sudo apt remove [nom_du_paquet]*** désinstalle un paquet, et ***sudo apt purge [nom_du_paquet]*** supprime également les fichiers de configuration associés.
- **Nettoyage des paquets inutiles :** ***sudo apt autoremove*** aide à nettoyer le système des paquets devenus inutiles après une mise à jour ou une désinstallation.

Kali Linux dispose de dépôts spécialisés pour les outils de test de pénétration, assurant que les utilisateurs ont accès aux dernières versions des outils de sécurité.

3.3. Similitudes dans l'Utilisation de APT

3.3.1. Commandes de base

Les commandes de base pour utiliser **APT** sont identiques dans **Parrot OS** et **Kali Linux**, étant donné qu'elles sont basées sur **Debian**. Les commandes suivantes sont couramment utilisées dans les deux distributions :

- **sudo apt update** : Met à jour la liste des paquets disponibles à partir des dépôts configurés.
- **sudo apt upgrade** : Met à jour les paquets installés vers leurs versions les plus récentes disponibles.
- **sudo apt install [nom_du_paquet]** : Installe un nouveau paquet.
- **sudo apt remove [nom_du_paquet]** : Supprime un paquet installé.
- **sudo apt purge [nom_du_paquet]** : Supprime un paquet installé et ses fichiers de configuration.
- **sudo apt autoremove** : Supprime les paquets qui ne sont plus nécessaires.

Ces commandes offrent une méthode standardisée et efficace pour gérer les logiciels sur les deux systèmes.

3.3.2. Gestion des dépôts

Les deux distributions utilisent des fichiers de configuration pour gérer les dépôts de logiciels. Les fichiers **/etc/apt/sources.list** et **/etc/apt/sources.list.d/** contiennent les informations sur les dépôts. Les utilisateurs peuvent ajouter des dépôts tiers en modifiant ces fichiers, ce qui permet l'installation de logiciels supplémentaires non inclus dans les dépôts officiels.

Les dépôts de **Parrot OS** et **Kali Linux** sont configurés pour fournir les paquets spécifiques à leurs besoins. Les utilisateurs peuvent également ajouter des dépôts tiers pour accéder à des logiciels supplémentaires, en modifiant les fichiers de configuration des dépôts.

3.4. Différences dans l'utilisation de APT

3.4.1. Dépôts Spécifiques

- **Parrot OS :**
    - Inclut des dépôts spécialement conçus pour des outils axés sur la confidentialité et l'anonymat, en plus des outils de sécurité standards. Ces dépôts offrent une sélection de logiciels orientés vers la protection de la vie privée et l'anonymat, comme **Anonsurf, Tor**, et divers outils de cryptage.
    - Les dépôts de **Parrot OS** sont configurés pour fournir des mises à jour régulières des outils de sécurité et de confidentialité, garantissant que les utilisateurs ont accès aux dernières versions des logiciels.
- **Kali Linux :**
    - Maintien des dépôts spécifiques pour les outils de test de pénétration et de sécurité. **Kali Linux** met l'accent sur la fourniture des dernières versions des outils de sécurité, souvent bien avant qu'ils ne soient disponibles dans les dépôts standards de **Debian**.
    - Les dépôts de Kali Linux sont optimisés pour inclure des outils de sécurité, de forensique, et de test de pénétration. **Kali** offre également des paquets spécifiques pour des scénarios particuliers, comme les métapaquets **kali-linux-top10** qui incluent les dix outils les plus utilisés.

3.4.2. Scripts et Automatismes

- **Parrot OS :**
    - Inclut des scripts et des outils pour faciliter la configuration des outils de confidentialité. Par exemple, **Anonsurf** peut être installé et configuré via des commandes simples, ce qui automatise le processus de configuration du routage de trafic via **Tor.**
    - **Parrot OS** propose également des outils pour le cryptage des fichiers, la gestion des mots de passe, et la suppression sécurisée des données, intégrés directement dans les dépôts et faciles à installer via **APT**.
- **Kali Linux :**
    - Propose des **métapaquets** comme **kali-linux-top10** et **kali-linux-all** qui permettent aux utilisateurs d'installer rapidement un ensemble d'outils

préconfigurés pour différents scénarios de tests de pénétration. Ces **métapaquets** simplifient l'installation et la configuration des outils les plus couramment utilisés par les professionnels de la sécurité.

- **Kali Linux** inclut également des scripts automatisés pour configurer des environnements de test spécifiques, comme les environnements virtuels pour des exercices de **capture the flag (CTF)** et des simulations d'attaques.

3.5. Gestion des dépendances et des conflits

- **Parrot OS**

Parrot OS, grâce à sa base Debian, utilise **APT** pour gérer les dépendances et les conflits entre les paquets. Lorsqu'un utilisateur installe un nouveau paquet, **APT** résout automatiquement les dépendances requises, garantissant que tous les composants nécessaires sont installés. En cas de conflit, **APT** propose des solutions ou des alternatives pour résoudre le problème.

- **Kali Linux**

Kali Linux utilise également **APT** pour la gestion des dépendances, avec une attention particulière aux outils de sécurité. **Kali** veille à ce que les versions les plus récentes et les plus compatibles des outils de sécurité soient disponibles, minimisant les conflits et garantissant la stabilité du système. En cas de conflit, les mainteneurs de **Kali** fournissent souvent des correctifs ou des instructions spécifiques pour résoudre les problèmes.

Chapitre 3 : Comparaison entre les outils de sécurité de Kali Linux et Parrot OS

1. Introduction

1.1. Les versions des OS utilisés dans cette étude

- **Kali Linux :** ***"kali-rolling 2024.1"***

Figure 3 : *Version de Kali Linux Utilisée pour cette étude*

- **Parrot OS:** ***"Parrot Security 6.0 (lorikeet)"***

Figure 4 : *Version du* ***Parrot OS*** *utilisée pour cette étude*

1.2. Approche

Dans cette étude comparative, nous nous concentrerons sur deux aspects principaux :

- **Les catégories :**

Nous comparerons les catégories existantes dans chaque distribution, pour déterminer si elles couvrent tous les volets nécessaires pour le cyber sécurité

- **Les outils dans chaque catégorie :**

Nous effectuerons une comparaison plu approfondie au niveau des outils présents dans chaque catégorie au sein de chaque distribution, puis nous tenterons de regrouper les outils similaires disponibles à la fois dans les 02 distributions.

2. Comparaison au niveau des catégories

Nous avons constaté qu'une catégorie, **"Database Assessment"** est présente sur **Kali Linux** mais absente sur **Parrot OS.**

De même, les catégories **"Automotive"** et **"Privacy"** sont disponibles sur **Parrot OS** mais absentes sur **Kali Linux**.

Par ailleurs, certaines catégories sont équivalentes entre les deux distributions : par exemple, les catégories **"Post Exploitation"** et **"Maintaining Access"** de **Parrot OS** correspondent à la catégorie **"Post Exploitation"** de **Kali Linux**. De plus, la catégorie **"Social Engineering"** de **Kali Linux** n'est qu'une sous-catégorie dans **Parrot OS.**

- **Catégories d'outils dans Kali Linux :**

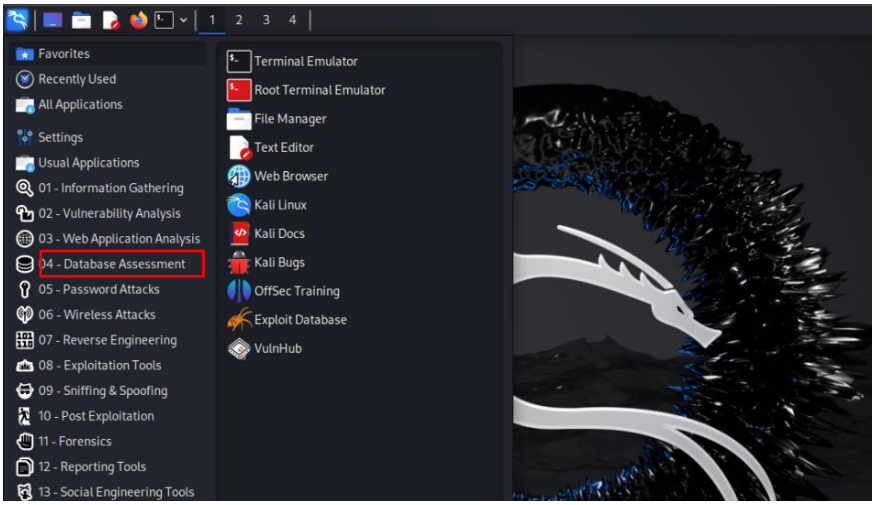

Figure 5 : *Catégories d'outils dans Kali Linux*

- **Catégories d'outils dans Parrot OS :**

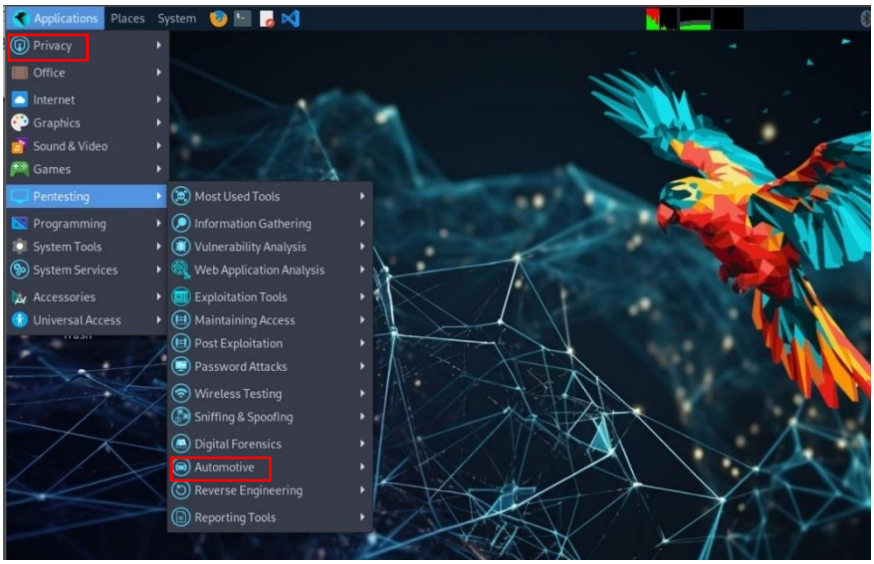

Figure 6 : *Catégories d'outils dans* ***Parrot OS***

Kali Linux	Parrot OS
Information Gathering	Information Gathering
Vulnerability Analysis	Vulnerability Analysis
Web Application Analysis	Web Application Analysis
Database Assessment	
Password Attacks	Password Attacks
Wireless Attacks	Wireless Testing
Reverse Engineering	Reverse Engineering
Exploitation Tools	Exploitation Tools
Sniffing & Spoofing	Sniffing & Spoofing
Post Exploitation	Post Exploitation
	Maintaining Access
Forensics	Digital Forensics
Reporting Tools	Reporting Tools
Social Engineering	C'est une sous-catégorie dans la catégorie **Exploitation Tools**
	Automative
	Privacy

Tableau 1 : *Comparaison des catégories entre Kali Linux et* ***Parrot OS***

Donc, pour unifier l'étude comparative des outils, nous nous concentrerons sur les catégories présentes sur les 02 distributions à la fois, et qui sont :

- **Information Gathering :**

Contient des outils conçus pour la collecte, l'organisation et l'analyse de données et de renseignements sur une cible, telle qu'un réseau informatique, un site Web ou un individu, afin d'identifier les vulnérabilités qui peuvent être utilisées à des fins de recherche, d'analyse des menaces, de planification stratégique ou exploitées à des fins offensives et/ou opérations défensives.

- **Vulnerability Analysis :**

Comporte des outils qui pour but de tester, identifier et attribuer des niveaux de gravité à autant de défauts de sécurité que possible dans un délai donné.

- **Web Application Analysis :**

Contient des outils qui se concentrent sur l'évaluation de la sécurité d'une application Web. Le processus implique une analyse active de l'application pour détecter toute faiblesse, défaut technique ou vulnérabilité.

- **Password Attacks :**

Comporte des outils qui aident à amener différents types d'attaques de mots de passe, comme : le brute forcing, en utilisant keylogger ou des dictionnaires, tout dans le but de trouver de mots de passe vulnérables pour accéder à un système.

- **Wireless Attacks :**

Comporte une variété d'outils qui aident a amener des actions délibérées et malveillantes visant à exploiter les vulnérabilités des systèmes de communication sans fil pour obtenir un accès non autorisé, intercepter des données sensibles, perturber les opérations du réseau ou compromettre la sécurité des appareils et des utilisateurs connectés au réseau.

- **Reverse Engineering :**

Outils qui ont la capacite de démonter un objet / système pour voir comment il fonctionne en interne, dans le but d'analyser et d'acquérir des connaissances sur le fonctionnement interne du système.

- **Exploitation Tools :**

Comporte des outils conçus pour exploiter les vulnérabilités trouvées dans un système afin de gagner un accès illégal.

- **Sniffing & spoofing :**

Ensemble d'outils permettant de surveiller tous les paquets de données transitant sur le réseau, et d'autre qui aident à introduire un faux trafic et prétend être quelqu'un d'autre (source légale ou entité légitime) dans le but d'usurper l'identité de quelqu'un.

- **Post Exploitation :**

Outils aident à maintenir l'accès au système an utilisant des backdoors ...etc, ou effectuer des mouvements latéraux...etc.

- **Digital Forensics :**

Englobe les outils utiles pour l'identification, l'acquisition, le traitement, l'analyse et le reporting des données stockées électroniquement.

- **Reporting Tools :**

Ce sont des outils qui aident a documenter les trouvailles et présenter les informations d'une manière facile à comprendre.

3. Comparaison au niveau des outils de sécurité

Après avoir unifié les catégories entre les deux distributions, nous avons effectué une comparaison des outils présents dans chaque catégorie. Enfin, nous avons regroupé les outils similaires entre **Kali Linux** et **Parrot OS.**

3.1. Information Gathering

	dmitry
	ike-scan
	netdiscover
	nmap
	recon-ng
DNS Analysis	
	dnsenum
IDS/IPS Identification	
	lbd
	wafw00f
Live Host Idnetification	
	arping
	fping
	hping3
	thcping6
Network & Port Scanners	
	masscan
	nmap
OSINT Analysis	
	Theharvester
Route Analysis	
Parrot Only	intrace
Kali Only	netmask
SMB Analysis	
	enum4linux
	nbtscan
	smbmap
SMTP Analysis	
	swaks
SNMP Analysis	
	snmp-check
	onesixtyone
SSL Analysis	
	ssldump
	sslh
	sslscan

Tableau 2 : *Intersection des outils d'Information Gathering entre Kali Linux et Parrot OS*

3.2. Vulnerability Analysis

	unix-privesc-check
Fuzzing Tools	
	spike-generic_chunked
	spike-generic_listen_tcp
	spike-generic_send_tcp
	spike-generic_send_udp
VoIP Tools	
	voiphopper

Tableau 3 : *Intersection des outils de Vulnerability Analysis entre Kali Linux et Parrot OS*

3.3. Web Application Analysis

	commix
	sqlmap
CMS & Framework Identification	
Kali Only	wpscan
Parrot Only	joomscan
	wig
Web Application Proxies	
	Burpsuite
Web Crawlers & Directory Bruteforce	
	dirb
	dirbuster
	wfuzz
Web Vulnerability Scanners	
	davtest
	nikto
	skipfish
	whatweb

Tableau 4 *: Intersection des outils de Web App Analysis entre Kali Linux et Parrot OS*

3.4. Password Attacks

	hashid
Offline Attacks	
	chntpw
	hashcat
	John
	ophcrack CLI
	samdump2
Online Attacks	
	hydra
	medusa
	ncrack
	onesixtyone
	thc-pptp-bruter
Password Profiling & Wordlists	
	cewl
	crunch
	rsmangler
	wordlists

Tableau 5 : *Intersection des outils de Password Attacks entre Kali Linux et Parrot OS*

3.5. Wireless Testing

	aircrack-ng
	fern wifi cracker
	pixiewps
	reaver
	wifite
802.11 Wireless Tools	
	bully
Bluetooth Tools	
Kali Only	spooftooph
Parrot Only	crackle
	btscanner

Tableau 6 : *intersection des outils de Wireless Attacks entre Kali Linux et Parrot OS*

3.6. Reverse Engineering

	Ghidra
Kali Only	
	Clang
	Clang++
	NASM shell
Parrot Only	
Debuggers	edb-debugger
	GNU debugger
	Javasnoop
Decompilers	Dex2jar

Tableau 7 : *Intersection des outils de Reverse Engineering entre Kali Linux et Parrot OS*

3.7. Exploitation Tools

	Metasploit framework
	Social engineering toolkit
	sqlmap

Tableau 8 : *Intersection des outils d'Exploitation Tools entre Kali Linux et Parrot OS*

3.8. Sniffing & Spoofing

	ettercap
	macchanger
	mitmproxy
	responder
	wireshark
Network Sniffers	
	netsniff-ng
Spoofing & MITM	
	dnschef
	rebind
	sslsplit
	tcpreplay

Tableau 9 : *Intersection des outils de Sniffing & Spoofing entre Kali Linux et Parrot OS*

3.9. Post Exploitation Tools

	mimikatz
	powersploit
	powershell empire
OS Backdoors	
	sbd
Tunneling & Exfiltration	
	dns2tcpc
	dns3tcpd
	iodine
	miredo
	proxychains
	proxytunnel
	ptunnel
	pwnat
	sslh
	stunnel4
	udptunnel
Web Backdoors	
	laudanum
	weevely

Tableau 10 : *Intersection des outils de Post Exploitation entre Kali Linux et Parrot OS*

3.10. Digital Forensics

	autopsy
	binwalk
	hashdeep
Forensics Carving Tools	
	magicrescue
	scalpel
	scrounge-ntfs
Forensic Imaging Tools	
	guymager
PDF Forensics Tools	
	pdfid
	pdf-parser
Sleuth Kit Suite	

Tableau 11 : *Intersection des outils de Forensics entre Kali Linux et Parrot OS*

3.11. Reporting Tools

Parrot Only	
	eyewitness
Kali Only	
	cherrytree
	cutycapt
	pipal
	recordmydesktop

Tableau 12 : *Intersection des outils de Reporting entre Kali Linux et Parrot OS*

4. Conclusion de Comparaison

En examinant les intersections des outils de chaque catégorie entre Kali Linux et **Parrot OS,** nous constatons que les outils similaires entre les deux distributions sont **les outils les plus populaires et plus utilisés** par les professionnels et les chercheurs en cyber sécurité, on cite parmi eux :

nmap, wireshark, mimikatz, powershell empire, metasploit framework , sqlmap, autopsy, aircrack-ng, hydra, hashcat, Burpsuite, theharvester, nikto ...etc

Ce qui témoigne une similitude d'orientation sécurité entre les deux distributions, et que les deux offrent un package d'outils principaux appropriées pour les débutants et les professionnels en cyber sécurité.

Cependant, il y a des différences au niveau d'autres outils et des catégories assez importants, ce qui peut être expliquée par une différence des préférences et des philosophies distincts :

- **Kali Linux** est conçu principalement pour les tests d'intrusions professionnels et l'audit de sécurité ce qui rend L'accent plus fort sur l'offre d'un ensemble complet d'outils pour les pentesters et les professionnels de la cybersécurité.

- Alors que **Parrot OS** est conçu pour être polyvalent, avec un accent sur la sécurité, la confidentialité et l'anonymat, donc il vise à offrir un environnement plus axé sur la protection des utilisateurs au quotidien, en plus des tests de sécurité.

Chapitre 4 : Proposition d'une panoplie personnalisée de sécurité

Chaque organisation ou individu a des besoins spécifiques en matière de sécurité, dictés par des facteurs tels que l'environnement de travail, les types de données manipulées et les menaces potentielles auxquelles ils sont exposés.

Cette section vise à proposer une panoplie de sécurité personnalisée, sélectionnée selon des critères rigoureux.

En combinant les outils les plus performants de **Kali Linux** et de **Parrot OS,** notre objectif est de créer une suite de sécurité qui maximise les avantages des deux distributions tout en minimisant leurs limitations respectives.

1. Critères de sélection des outils

1.1. Efficacité et Performance

C'est le critère le plus important, pour avoir une expérience optimale, on doit choisir des outils qui sont efficaces, rapides, précis dans la réalisation de leurs tâches et qui fonctionnent de manière optimale sans dégrader les performances globales du système.

1.2. Facilite d'utilisation

La simplicité de l'interface utilisateur, la facilité de configuration et d'utilisation et la disponibilité de documentation et de support utilisateur, sont tous des critiques à vérifier avant de sélectionner l'outil.

1.3. Flexibilité et polyvalence

L'outil qui couvre plusieurs fonctionnalités et qui peut être adapté à différents scénarios de sécurité est souvent le plus approprié. Il offre la plupart des exigences de sécurité nécessaires dans une seule interface, aidant ainsi à éviter le gaspillage des ressources physiques qui résulterait du téléchargement de multiples outils pour chaque fonctionnalité.

1.4. Mises à jour et support technique

Fréquence et régularité des mises à jour et des améliorations ainsi la disponibilité des patchs de sécurité et des supports techniques sont très importants pour la sélection de l'outils.

1.5. Couts

La disponibilité des versions gratuites et open sources est très important surtout pour les étudiants et les débutants qui ne serons pas sure au début de ce qu'ils veulent et tenterons plusieurs choix en premier avant de décider les meilleurs outils à utiliser.

1.6. Réputation et communauté

La réputation et la taille de communauté disponible pour l'outil peut faire une différence lors de la sélection, la disponibilité d'une communauté large et active est très importante pour recevoir le soutien et le support nécessaire.

2. Sélection des meilleurs outils de chaque distribution

2.1. Introduction

Nous avons essayé de regrouper tous les outils qui se conforment avec les critères cités avant, ainsi nous avons pris en considération notre expertise personnelle avec chaque outil, et plus important nous avons tenté de regrouper les outils qui vont couvrir le maximum possible des volets de sécurité nécessaires.

2.2. Panoplie personnalisée : Outils choisis

Information Gathering	
	dnsenum
	enum4linux
	nmap
	recon-ng
	Theharvester
Vulnerability Analysis	
	nikto
	unix-privesc-check
	OpenVas
Web Application Analysis	
	Burpsuite
	dirbuster
	Zap proxy
	skipfish
	sqlmap
Password Attacks	
	cewl
	hashcat
	hydra
	John
	medusa
	wordlists
Wireless Testing	
	aircrack-ng
	bully
	crackle
	pixiewps
	reaver
	wifite
Reverse Engineering	
	dex2jar
	edb-debugger
	Ghidra
	javasnoop
Exploitation Tools	
	armitage
	metasploit Framework

	social engineering toolkit
	sqlmap
Sniffing & Spoofing	
	dnschef
	mitmproxy
	responder
	sslsplit
	wireshark
Post Exploitation	
	mimikatz
	powershell empire
	powersploit
	sbd
	weevely
Digital Forensics	
	autopsy
	Bulk Extractor
	guymager
	pdf-parser
	regripper
	Sleuth Kit Suite
Reporting Tools	
	Cherrytree

Tableau 13 : *Panoplie Personnalisée*

3. Intégration des outils sélectionnés dans Ubuntu 23.10

3.1. Katoolin3

Katoolin est un script Python écrit par **LionSec** pour installer les outils **Kali Linux** dans **Ubuntu, Debian** et d'autres systèmes basés sur **DEB**.

Il semble que **Katoolin** ne soit pas mis à jour régulièrement (le dernier commit date d'avril 2019) et cela ne fonctionne pas dans les versions récentes d'**Ubuntu**. Les mises en garde ont commencé à s'accumuler en raison du manque de maintenance.

Donc, quelqu'un a repris le flambeau et lancé **Katoolin3**, un fork de **Katoolin** utilisant **Python3** au lieu de **Python 2** et il est mis à jour et plus stable que l'ancienne version

3.1.1. Limitations du Katoolin3

Il semble qu'aussi **Katoolin3** n'est pas mis à jour et souffre de plusieurs problèmes, en commençant par l'installation, **katoolin3** aujourd'hui ne peut être installé sur **Ubuntu** jusqu'à ce qu'on change la clé **GPG** utilisée par le script de l'installation **(install.sh)**

Ainsi Il semble que **Katoolin3** gâche les référentiels existants. De nombreux utilisateurs se sont plaints du fait que **Katoolin3** supprime **GNOME DE** et d'autres packages qui ne sont même pas liés à **Katoolin** lorsqu'ils tentent de désinstaller **Katoolin**.

Donc il n'est jamais recommandé d'utiliser **Katoolin3** sur une vraie machine !!

3.1.2. Installation du Katoolin3

On clone le répertoire **GitHub** où réside **Katoolin3** sur notre machine :

git clone https://github.com/s-h-3-l-l/katoolin3;
cd katoolin3;
chmod +x ./install.sh;
sudo ./install.sh;

En exécutant ces commandes le répertoire va être copié, mais **Katoolin3** ne peut pas être installé, on doit d'abord ignorer la clé **GPG** utilisée par le script **install.sh** et télécharger une nouvelle clé de **kali** :

```
esma@esma-None:~$ wget -q -O - https://archive.kali.org/archive-key.asc | sudo apt-key add -
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
OK
```

```
esma@esma-None:~$ apt-key list
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
/etc/apt/trusted.gpg
--------------------
pub   rsa4096 2012-03-05 [SC] [expires: 2027-02-04]
      44C6 513A 8E4F B3D3 0875  F758 ED44 4FF0 7D8D 0BF6
uid           [ unknown] Kali Linux Repository <devel@kali.org>
sub   rsa4096 2012-03-05 [E] [expires: 2027-02-04]

/etc/apt/trusted.gpg.d/ubuntu-keyring-2012-cdimage.gpg
------------------------------------------------------
pub   rsa4096 2012-05-11 [SC]
      8439 38DF 228D 22F7 B374  2BC0 D94A A3F0 EFE2 1092
uid           [ unknown] Ubuntu CD Image Automatic Signing Key (2012) <cdimage@ubuntu.com>

/etc/apt/trusted.gpg.d/ubuntu-keyring-2018-archive.gpg
------------------------------------------------------
pub   rsa4096 2018-09-17 [SC]
      F6EC B376 2474 EDA9 D21B  7022 8719 20D1 991B C93C
uid           [ unknown] Ubuntu Archive Automatic Signing Key (2018) <ftpmaster@ubuntu.com>
```

Figure 7 : *Importation de nouvelle clé de Kali pour Katoolin3*

Maintenant on peut lancer et utiliser **Katoolin3** pour intégrer notre panoplie personnalisée dans **Ubuntu** :

```
esma@esma-None:~$ sudo katoolin3

 ~~~~~{ Author: s-h-3-l-l | Homepage: https://github.com/s-h-3-l-l }~~~~~

Hit:1 http://ma.archive.ubuntu.com/ubuntu mantic InRelease
Hit:2 http://security.ubuntu.com/ubuntu mantic-security InRelease
Hit:4 http://ma.archive.ubuntu.com/ubuntu mantic-updates InRelease
Hit:5 http://ma.archive.ubuntu.com/ubuntu mantic-backports InRelease
Get:3 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 Packages [19.2 MB]
Get:7 http://kali.download/kali kali-rolling/contrib amd64 Packages [114 kB]
Get:8 http://kali.download/kali kali-rolling/non-free amd64 Packages [192 kB]
Fetched 19.5 MB in 41s (478 kB/s)
Reading package lists...
W: http://http.kali.org/kali/dists/kali-rolling/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg),
ils.

DISCLAIMER:
Don't update your packages, upgrade your system or
modify your package cache in any other way while
katoolin3 is still running!

Main Menu
0) View Categories
1) Install All
2) Uninstall All
3) Search repository
4) List installed packages
5) List not installed packages
6) Install Kali Menu
7) Uninstall old katoolin
8) Help
9) Exit
```

Figure 8 : *Katoolin3 sur Ubuntu*

On suit la numérotation du menu pour visualiser et installer les catégories et leurs outils :

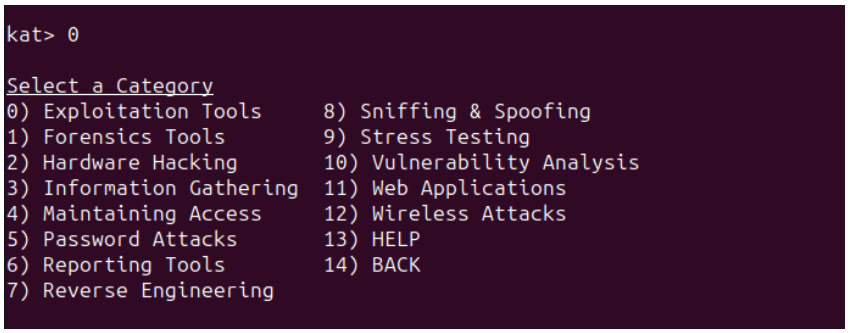

Figure 9 : *Les catégories dans Katoolin3*

3.2. Installation des outils sélectionnés sur Ubuntu selon la catégorie

On suit les numérotations pour accéder à chaque catégorie et installer chaque outil parmi ceux qu'on a déjà sélectionné

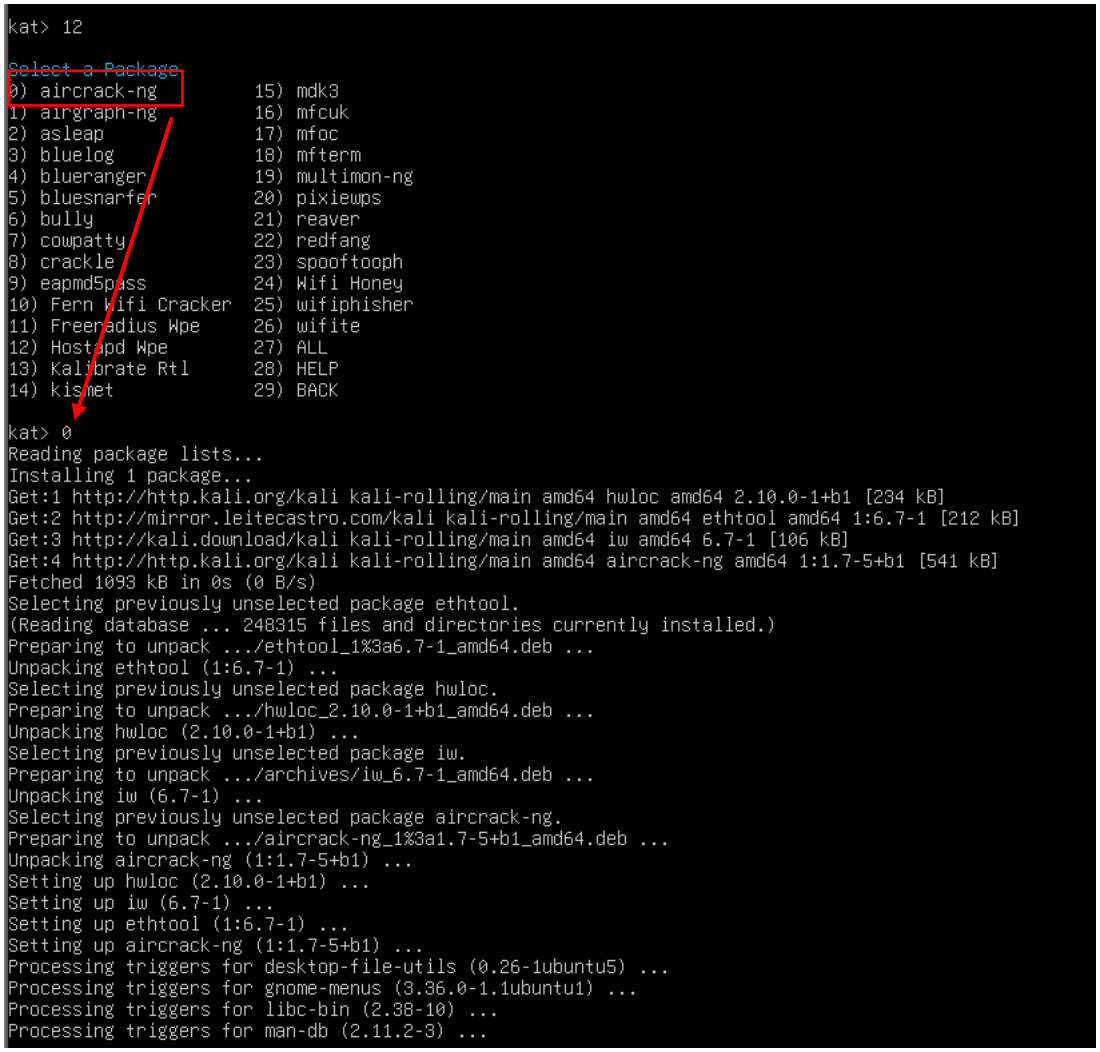

Figure 10 : *Comment les outils sont installés en utilisant Katoolin3*

NOTE : *Apres l'installation de quelques outils on a constaté l'absence d'interface graphique !!*

Les outils qui ont été installés seront marques en gris !!

3.2.1. Information Gathering

Figure 11 : *Intégration des outils d'Information Gathering dans Ubuntu 23.10*

3.2.2. Vulnerability Analysis

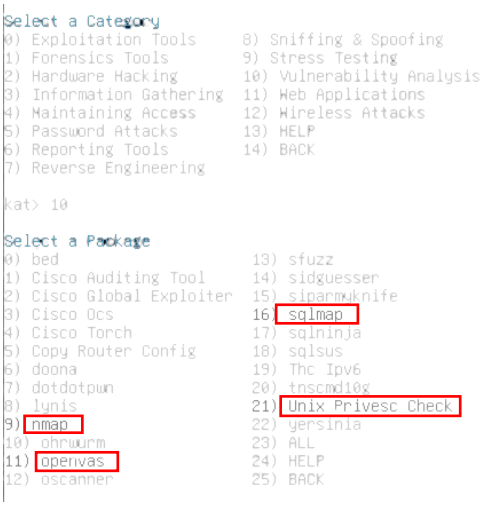

Figure 12 : *Intégration des outils de Vulnerability Analysis dans Ubuntu 23.10*

3.2.3. Web Application Analysis

Figure 13 : *Intégration des outils de Web App Analysis dans Ubuntu 23.10*

3.2.4. Passwords Attacks

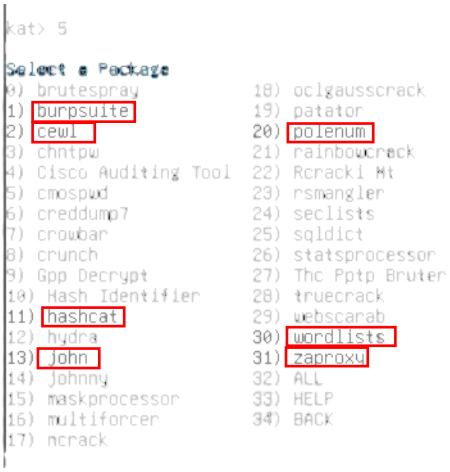

Figure 14 : *Intégration des outils de Password Attacks dans Ubuntu 23.10*

3.2.5. Wireless Attacks

Figure 15 : *Intégration des outils de Wireless Attacks dans Ubuntu 23.10*

3.2.6. Reverse Engineering

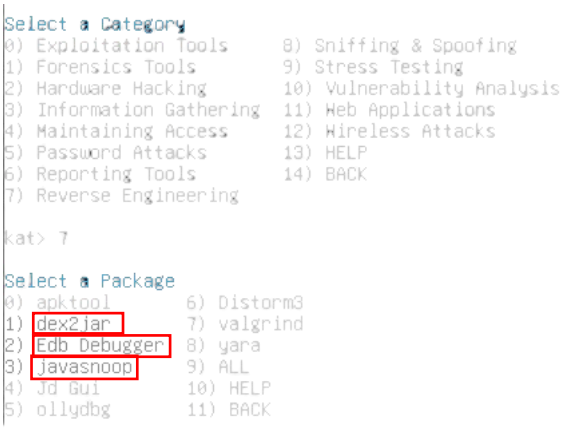

Figure 16 : *Intégration des outils de Reverse Engineering dans Ubuntu 23.10*

3.2.7. Exploitation Tools

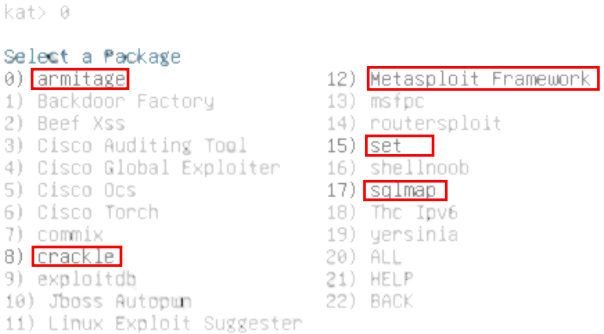

Figure 17 : *Intégration des outils d'exploitation dans Ubuntu 23.10*

3.2.8. Sniffing & Spoofing

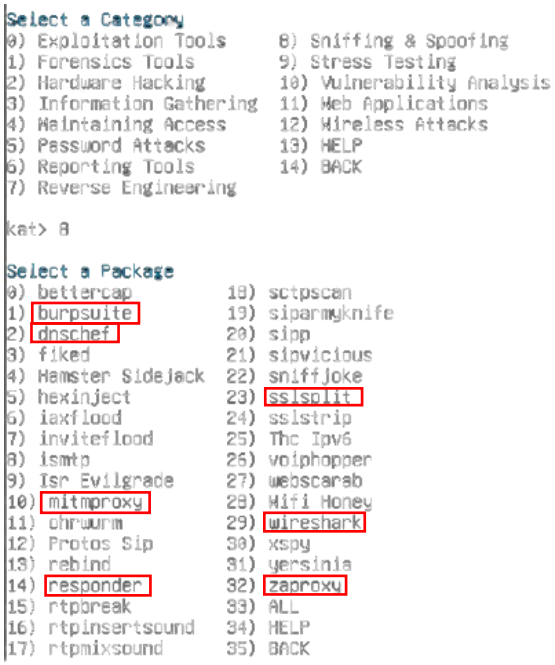

Figure 18 : *Intégration des outils de Sniffing & Spoofing dans Ubuntu 23.10*

3.2.9. Post Exploitation

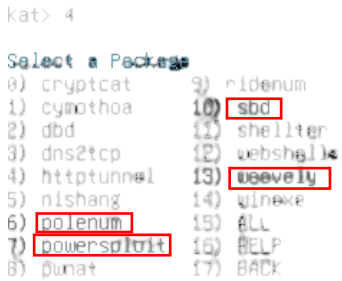

Figure 19 : *Intégration des outils Post exploitation dans Ubuntu 23.10*

3.2.10. Digital Forensics

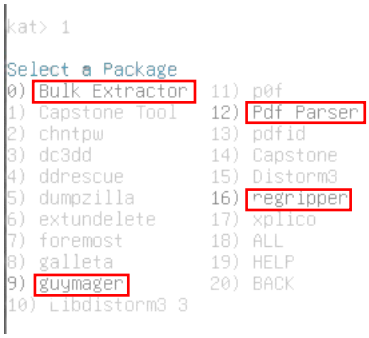

Figure 20 : *Intégration des outils d'analyse d'évidences dans Ubuntu 23.10*

3.2.11. Reporting Tools

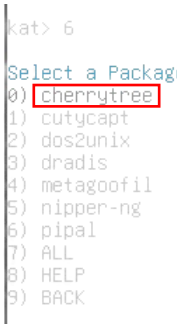

Figure 21 : *Intégration des outils de Reporting dans Ubuntu 23.10*

Conclusion

En conclusion, cette étude comparative entre **Kali Linux** et **Parrot OS** a permis de mettre en lumière les points forts et les différences clés de ces deux distributions axées sur la sécurité. Les outils communs tels que **nmap, wireshark, mimikatz**, et **metasploit** montrent une orientation similaire vers la sécurité, offrant un package robuste et complet pour les professionnels et les débutants en cybersécurité. Cependant, chaque distribution possède des outils uniques et des philosophies distinctes qui répondent à des besoins spécifiques.

Kali Linux se distingue par son focus sur les tests d'intrusion et l'audit de sécurité, en fournissant une panoplie exhaustive d'outils pour les pentesters. En revanche, **Parrot OS** se veut plus polyvalent, mettant l'accent sur la sécurité, la confidentialité et l'anonymat des utilisateurs au quotidien, en plus des tests de sécurité.

À travers ce rapport, nous avons également proposé une panoplie de sécurité personnalisée en combinant les outils les plus performants de chaque distribution. Cette approche vise à maximiser les avantages offerts par **Kali Linux** et **Parrot OS** tout en minimisant leurs limitations respectives. En tenant compte des critères de performance, de facilité d'utilisation, de flexibilité, de support technique et de coûts, nous avons sélectionné les outils les plus adaptés pour répondre aux différents scénarios de sécurité.

Cette étude et proposition d'outils devraient fournir aux professionnels de la sécurité informatique une ressource précieuse pour renforcer la protection de leurs systèmes et réseaux. En combinant le meilleur des deux mondes, nous espérons offrir une solution sur mesure qui répond efficacement aux besoins variés en matière de sécurité informatique dans un environnement numérique en constante évolution.

Webographie

Kali Linux – Wikipedia: https://fr.wikipedia.org/wiki/Kali_Linux (27/06/2024)

Kali Linux Blog : https://www.kali.org/blog/10-years/ (27/06/2024)

ParrotOS Documentation : https://parrotsec.org/docs/introduction/what-is-parrot/ (27/06/2024)

Parrot (machine virtuelle) – Wikipedia: https://fr.wikipedia.org/wiki/Parrot_(machine_virtuelle) (27/06/2024)

Difference between Kali Linux and Parrot OS – GeeksforGeeks: https://www.geeksforgeeks.org/difference-between-kali-linux-and-parrot-os/ (27/06/2024)

Kali Linux VS Parrot OS – Stationx : https://www.stationx.net/kali-linux-vs-parrot-os/ (27/06/2024)

Advanced Packaging Tool – Wikipedia: https://fr.wikipedia.org/wiki/Advanced_Packaging_Tool (27/06/2024)

Apt [Wiki ubuntu-fr]: https://doc.ubuntu-fr.org/apt (27/06/2024)

What is the apt system : https://web.archive.org/web/20171016084837/http://aptitude.alioth.debian.org/doc/en/pr01s03.html (27/06/2024)

Github – Katoolin3: https://github.com/s-h-3-l-l/katoolin3 (27/06/2024)

Install Kali Linux Tools Using Katoolin3 In Ubuntu 20.04 LTS : https://ostechnix.com/install-kali-linux-tools-using-katoolin3-in-ubuntu-20-04-lts/ (27/06/2024)