SEC-LEC : Durcissement sécurité Linux

Egersec Formation

Gérard Bigot

28/02/2022

Egersec Groupe

Egersec est une structure offrant à sa clientèle un ensemble de services autour du conseil, de la formation et de la sécurisation de Systèmes d'Informations.

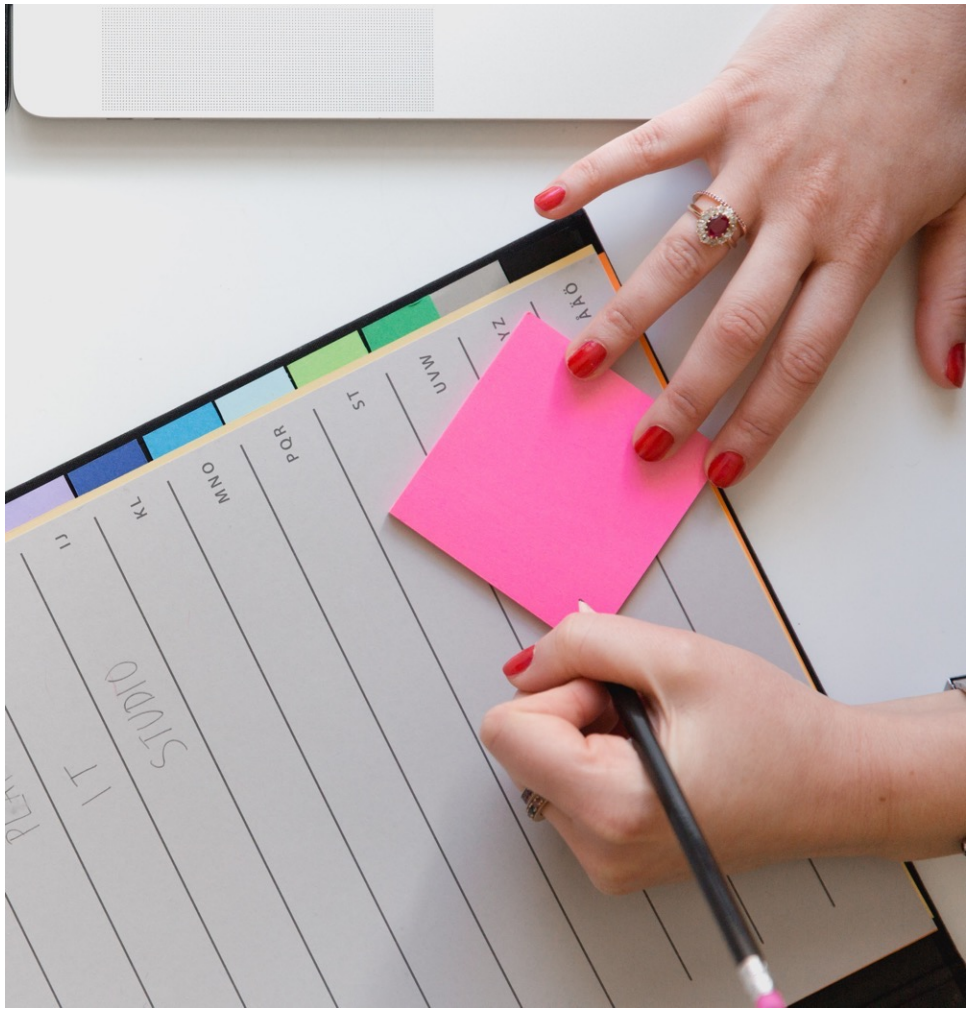
Nous sommes organisés autour de trois structures :

- Egersec Consulting qui fournit des prestations de conseil afin de protéger l'ensemble des actifs de l'entreprise.
- Egersec Cybersécurité qui propose des solutions pérennes d'installation et d'exploitation de la sécurité des actifs.
- Egersec Formation qui assure des prestations de formation à haute valeur ajoutée.

Nos expériences et notre histoire nous ont amené à combiner une forte approche de direction projet avec expertise des normes et méthode de sécurisation des actifs de l'entreprise.

Nos différentes offres s'adaptent aux besoins des petites et très petites entreprises. Elles commencent toutes par une journée d'audit et de compréhension des besoins, puis l'établissement d'une proposition en rapport avec le budget vs le niveau de sécurisation demandé.
Elle peut aller de la simple rédaction de procédures à la mise en place et l'exploitation d'un SOC complet.

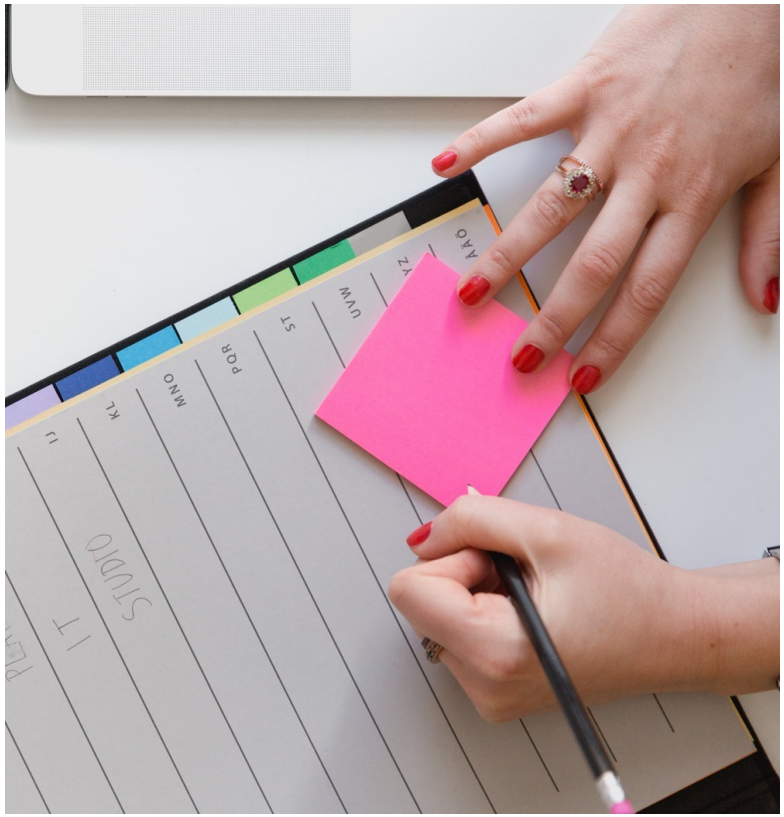
Fonctionnement de la session de formation:



- Posez des questions
- Interrompez le formateur si un point reste incompris
- Vos expériences personnelles concernant le sujet peuvent être intéressantes et donner lieu à un complément d'information
- Prenez en note les informations complémentaires fournies
- Le formateur reste le maître des horloges

Objectifs pédagogiques

L'objectif de ce cours est :



Identifier les principales menaces de l'environnement Linux et les différentes solutions qui s'y rapportent.

Optimiser la sécurisation du système.

Présentation des participants

Présentation de l'expérience du formateur et des élèves

- Votre nom, prénom
- Votre organisation
- Votre rôle

Qu'attendez-vous de cette formation ?

SEC-LEC : Durcissement sécurité Linux
Introduction

Multiplexed Information and Computing Service (Multics) était un système d'exploitation développé par les Bell Labs et d'autres institutions dans les années 1960 pour fournir un service informatique centralisé pour les utilisateurs. Multics était un système d'exploitation complexe qui a introduit de nombreuses innovations pour l'époque, notamment **la gestion de fichiers hiérarchiques, les processus en arrière-plan et le partage de ressources.**

Cependant, Multics était également très complexe et difficile à gérer, ce qui a entraîné des coûts élevés pour les utilisateurs. Ken Thompson, l'un des développeurs de Multics, a quitté le projet pour travailler sur un système d'exploitation plus simple appelé Unix.

Unix a été conçu pour fournir une solution plus simple et plus efficace aux utilisateurs qui souhaitaient un système d'exploitation multi-tâche et multi-utilisateur. Il a été influencé par de nombreux concepts de Multics, mais a également introduit de nouvelles idées pour améliorer la simplicité et l'efficacité du système.

Introduction - Généralités sur Linux - Historique

Unix est un système d'exploitation multi-utilisateur et multi-tâche créé au début des années 1970 par Ken Thompson et Dennis Ritchie au Bell Labs. Il a été conçu pour fournir aux scientifiques et aux ingénieurs un environnement de développement fiable et efficace pour les applications de programmation et de recherche.

Au fil des ans, Unix est devenu de plus en plus populaire et a été porté sur de nombreux matériels différents, ce qui a conduit à la création de nombreuses distributions Unix distinctes. Certaines de ces distributions, telles que AIX et Solaris, sont devenues des systèmes d'exploitation commerciaux, tandis que d'autres, telles que FreeBSD et NetBSD, sont devenues des systèmes d'exploitation libres et open-source.

L'influence d'Unix dans l'industrie des systèmes d'exploitation est considérable. De nombreux concepts clés d'Unix, **tels que les shells de commande, les pipes de redirection de fichiers et les processus en arrière-plan,** sont devenus des standards dans l'industrie des systèmes d'exploitation et sont encore utilisés aujourd'hui dans de nombreux systèmes d'exploitation modernes, y compris Linux et macOS.

Sous Unix, tout est traité comme un fichier.

Les périphériques de stockage tels que les disques durs et les clés USB, les entrées et sorties de données telles que les claviers et les écrans, les sockets de réseau, les processus en cours d'exécution, paramètres du kernel, etc., sont tous représentés sous forme de fichiers dans le système de fichiers.

Cette approche a plusieurs avantages :

- Permettre de gérer de manière uniforme différents types de données et de périphériques en utilisant les mêmes outils et les mêmes méthodes.
- Rendre le système plus flexible et plus facile à utiliser, car les utilisateurs peuvent travailler avec des périphériques de manière très similaire à la manière dont ils travaillent avec des fichiers ordinaires.
- Simplifier le développement de logiciels, car les développeurs peuvent utiliser les mêmes API pour accéder à différents types de périphériques et de données.

Introduction - Généralités sur Linux - Kernel

Linux a été créé en 1991 par **Linus Torvalds,** un étudiant finlandais en informatique à l'Université d'Helsinki.

À l'époque, Linus Torvalds cherchait à créer un noyau (ou cœur) de système d'exploitation pour son ordinateur personnel. Il voulait un **système d'exploitation qui puisse fonctionner sur un ordinateur à base d'Intel 80386** et qui soit semblable à Unix, mais plus simple et plus facile à utiliser.

Il a rapidement réussit à attirer l'attention de la communauté de développeurs de logiciels libres.

Le noyau Linux est aujourd'hui maintenu par une équipe de développeurs volontaires du monde entier, qui travaillent ensemble pour améliorer le noyau et le maintenir à jour.

Il est considéré comme l'un des noyaux de système d'exploitation **les plus stables et les plus fiables disponibles,** et il est utilisé dans de nombreux types d'appareils, des ordinateurs de bureau aux smartphones et aux serveurs de grande envergure.

SEC-LEC : Durcissement sécurité Linux

Introduction - Généralités sur Linux - GNU

GNU/Linux est un système d'exploitation basé sur Unix, qui a été développé par la Free Software Foundation (FSF) dans les années 1980. Le but de la FSF était de créer un système d'exploitation libre et open-source, qui puisse être utilisé, modifié et distribué librement par n'importe qui.

GNU/Linux est un système d'exploitation complet, qui comprend un ensemble d'outils et de logiciels qui permettent aux utilisateurs de faire tourner leurs ordinateurs et de les utiliser pour effectuer des tâches telles que la navigation sur le web, la création de documents, la programmation, etc.

Le système d'exploitation GNU/Linux est souvent appelé simplement "Linux", bien qu'il soit composé de deux parties distinctes : le noyau Linux, qui est le cœur du système d'exploitation, et l'ensemble d'outils et de logiciels du projet GNU, qui forment le reste du système d'exploitation.

GNU/Linux est largement utilisé dans les environnements de serveur et de développement, en raison de sa fiabilité, de sa stabilité et de ses coûts réduits. Il est également utilisé dans les systèmes embarqués, les appareils mobiles, les **supercalculateurs** et d'autres applications pour lesquelles un système d'exploitation fiable et personnalisable est nécessaire.

Introduction - Généralités sur Linux - Distributions

Les distributions Linux sont des versions prépackagées et personnalisées du système d'exploitation GNU/Linux. Elles comprennent le noyau Linux, ainsi que des applications et des utilitaires qui sont sélectionnés et configurés pour remplir des fonctions spécifiques.

Il existe de nombreuses distributions Linux, chacune ayant ses propres caractéristiques et fonctionnalités. Certaines distributions sont conçues pour être facilement utilisables par les utilisateurs non informatiques, tandis que d'autres sont destinées aux professionnels de l'informatique et aux développeurs.

Certaines distributions sont conçues pour être légères et rapides, ce qui les rend idéales pour les ordinateurs plus anciens ou pour les appareils mobiles, tandis que d'autres sont conçues pour offrir une large gamme de fonctionnalités pour les utilisateurs plus avancés.

Quelques exemples de distributions Linux populaires incluent Ubuntu, Fedora, Rocky Linux, Debian, Mint, Manjaro ou Slackware.

Introduction - Généralités sur Linux - Fixed Release

Les distributions Linux avec une sortie fixe (ou "**fixed release**") sont celles qui publient des versions stables à des intervalles de temps prédéterminés, généralement une à deux fois par an.

Ce genre de distributions met l'accent sur la stabilité et la fiabilité, et vise à fournir une plate-forme fiable pour les utilisateurs qui ne souhaitent pas être constamment perturbés par des mises à jour et des correctifs de sécurité.

Les utilisateurs peuvent savoir à quoi s'attendre en termes de fonctionnalités et de support, car les mises à jour importantes ne sont publiques qu'une fois par an ou tous les deux ans.

Les distributions en temps fixe incluent, entre autres, Red Hat Enterprise Linux, Ubuntu et SUSE Linux Enterprise Server. Elles sont souvent utilisées par les entreprises et les organisations qui nécessitent une plate-forme fiable et pérennes pour leurs applications critiques.

Les versions stables sont généralement soutenues pendant plusieurs années, ce qui permet aux utilisateurs de planifier les mises à niveau et les migrations de manière plus efficace.

Introduction - Généralités sur Linux - Rolling Release

A l'inverse, les distributions en temps libre (ou **"rolling release"**) publient des mises à jour plus fréquentes pour inclure des correctifs de sécurité, des mises à jour de logiciels et de nouvelles fonctionnalités.

Ce genre de distributions met l'accent sur la dernière technologie et les nouvelles fonctionnalités, mais peut parfois entraîner des problèmes de compatibilité ou des bugs si les mises à jour ne sont pas effectuées correctement.

Les distributions en temps libre incluent, entre autres, Arch Linux, Manjaro et Gentoo.

Elles sont souvent utilisées par les développeurs et les utilisateurs avancés qui souhaitent avoir accès aux dernières technologies et fonctionnalités rapidement.

Introduction - Généralités sur Linux - Gestionnaire de Paquet

Un **gestionnaire de paquets** est un logiciel qui permet d'installer, de mettre à jour et de désinstaller facilement des logiciels sur un système Linux. Il gère les dépendances, ce qui signifie que si une application dépend d'autres paquets pour fonctionner correctement, le gestionnaire de paquets les installera automatiquement. Cela peut économiser beaucoup de temps et d'efforts par rapport à l'installation manuelle des logiciels nécessaires.

Les gestionnaires de paquets les plus courants sont **apt** pour Debian et ses dérivées, et **dnf** pour Red Hat et ses dérivées.

Les repositories sont des serveurs en ligne qui stockent les paquets Linux. Les gestionnaires de paquets s'y connectent pour télécharger et installer les paquets requis. Ils peuvent inclure des paquets pour différentes versions d'un système d'exploitation, ainsi que des mises à jour de sécurité, des correctifs de bugs et des nouvelles versions de logiciels.

Les repositories sont généralement hébergés par les éditeurs de distributions Linux, mais il existe également des repositories tiers qui peuvent être ajoutés à un système pour fournir des paquets supplémentaires. Les utilisateurs peuvent en ajouter ou supprimer pour personnaliser leur installation de Linux et installer les paquets qui répondent le mieux à leurs besoins.

En utilisant les repositories associés aux gestionnaires de paquets, les utilisateurs peuvent garantir qu'ils obtiennent les paquets les plus récents et les plus sécurisés pour leur système Linux, ce qui peut être particulièrement important pour les systèmes utilisés pour des applications critiques.

Tout ceci peut signifier que les repositories d'une distribution représente une faiblesse dans la sécurité des Linux liés à ces repositories.

En effet, toute personne capable de prendre la main soit sur les serveurs qui servent ces paquets, soit sur les paquets pendant qu'ils viennent chez vous (les sites officiels de ubuntu sont uniquement accessible en http, par exemple) peut en modifier le contenu.

Les gestionnaires de ces dépôts en sont conscients, c'est la raison pour laquelle tout les paquets qu'ils produisent sont signés avec des certificats dédiés au repository lié. Le gestionnaire de paquet gère le contrôle de validité entre la signature et ce qu'il connait du certificat pour chaque paquet qu'il télécharge. S'assurant ainsi de son authenticité.

Pour parer aux problèmes de DDoS, et peut-être aussi aux problèmes financiers liés à la mise en place d'une grappe de serveurs capables de soutenir la charge de tout les downloads de la distribution, un ensemble de miroirs répartis à travers le monde a été mise place.

SEC-LEC : Durcissement sécurité Linux

Introduction - Menaces et attaques sur l'environnement Linux

Comme tout autre système d'exploitation, Linux est vulnérable à certaines menaces et attaques. Certaines des menaces les plus courantes pour les environnements Linux sont les suivantes :

- **Malware**: Les virus, chevaux de Troie et autres formes de malware peuvent affecter les systèmes Linux, bien que la popularité relativement faible de Linux par rapport à d'autres systèmes d'exploitation tels que Windows signifie qu'ils sont généralement moins ciblés par les cybercriminels
- **Piratage de comptes** : Vol d'information d'identification en utilisant la force brute pour deviner les mots de passe, ou en utilisant des exploits pour découvrir les informations d'identification
- **Exploits de vulnérabilité de logiciel** : Profitent de failles de sécurité dans des logiciels pour prendre le contrôle d'un système ou accéder à des données sensibles
- **Ransomware** : Prise en otage des données d'une entreprise contre rançon en les chiffrant
- **Attaques par déni de service (DoS)** : Visent à rendre un système ou un service inaccessible en envoyant une quantité excessive de trafic à un système ou en surchargeant les ressources du système
- **Advanced Persistent Threat (APT)** : Vise précisément les données d'une organisation, et peut passer plusieurs mois avant d'atteindre son objectif. Type d'attaque lent, mais à forte récompense potentielle.

OWASP Top Ten est une liste maintenue par l'OWASP (Open Web Application Security Project) qui classe les principales sources de problèmes que les logiciels possèdent. Et donc les points sur lesquels il faut faire attention.

Introduction - Menaces et attaques sur l'environnement Linux - CVE

Common Vulnerabilities and Exposures (CVE) est une liste de référence de vulnérabilités de sécurité connues, qui peut inclure des vulnérabilités dans des systèmes d'exploitation tels que Linux.

Les CVE sont également utilisées pour suivre les vulnérabilités de sécurité connues dans les applications sous Linux.

Les CVE sont généralement préfixées par "CVE-201<année>-<numéro de référence>", où l'année fait référence à l'année de publication de la CVE.

Par exemple, la CVE-2019-11477 est une vulnérabilité connue du noyau Linux qui a été publiée en 2019.

Vous pouvez trouver une liste complète de CVE pour Linux et ses applications sur le site web de Mitre, qui est responsable de la coordination de la numérotation des CVE.

SEC-LEC : Durcissement sécurité Linux

Introduction - La sécurité de l'environnement Linux - Sécurité de base

Les distributions Linux sont livrées avec un certain nombre d'outils de sécurité de base pour aider à protéger les systèmes contre les menaces et les attaques malveillantes.

Voici un choix de sécurisation de base communs que vous pouvez trouver dans la plupart des distributions Linux :

- **Pare-feu** : La plupart des distributions Linux sont livrées avec un pare-feu configuré par défaut, tel que iptables et/ou nftables, pour limiter l'accès au système depuis le réseau.
- **Contrôle d'accès** : Les distributions Linux disposent également de contrôles d'accès pour limiter l'accès aux ressources système et aux fichiers en fonction des privilèges de l'utilisateur.
- **Mises à jour de sécurité** : Les distributions Linux sont régulièrement mises à jour avec des correctifs de sécurité pour combler les vulnérabilités connues et protéger les systèmes contre les menaces. Il est important de maintenir le système à jour en installant régulièrement ces mises à jour.
- **Politiques de mot de passe** : Les distributions Linux disposent de politiques de mot de passe configurables qui peuvent renforcer la sécurité des comptes utilisateur en limitant la complexité et la durée de validité des mots de passe.
- **Surveillance du système** : Les outils de surveillance du système tels que l'audit de sécurité, les journaux système et les outils de surveillance du réseau sont également disponibles pour aider à identifier et à résoudre les problèmes de sécurité.
- **Sécurisation des connexions réseau** : Les distributions Linux sont livrées avec des outils tels que SSH pour permettre des connexions réseau sécurisées entre les systèmes.

SEC-LEC : Durcissement sécurité Linux

Introduction - La sécurité de l'environnement Linux - Pile d'outils pour faire un Firewall

Un **firewall** est un système de sécurité qui permet de contrôler les flux de données entrants et sortants d'un réseau, afin de protéger les ordinateurs et les données qui y sont stockées.

Linux propose une pile de solutions qui concourent à la mise en place d'un firewall efficace :

- Netfilter : C'est le firewall inclus dans le noyau Linux. Il permet de filtrer les paquets réseau en fonction de différentes règles définies par l'utilisateur. Netfilter peut être configuré en ligne de commande, mais il est plus courant de l'utiliser avec une interface graphique.
- **iptables/nftables** : iptables est l'outil en ligne de commande pour configurer Netfilter. Il permet de configurer des règles de filtrage en fonction de différents critères tels que l'adresse IP, le port, le protocole, etc. Nftables est une évolution d'iptables, qui propose une syntaxe simplifiée et une meilleure performance.
- **ufw** : ufw (Uncomplicated Firewall) est une interface simplifiée pour iptables. Il permet de configurer facilement un firewall en utilisant des règles prédéfinies pour différents services. ufw peut être configuré en ligne de commande ou via une interface graphique.
- **firewalld** : firewalld est un outil de gestion de firewall pour les distributions Linux utilisant Systemd. Il propose une approche plus dynamique du firewall, avec des zones prédéfinies pour différents types de réseaux et des règles appliquées en temps réel. Il dispose également d'une interface graphique pour simplifier la configuration.

Ces différents outils peuvent être utilisés selon les besoins de l'utilisateur et le niveau de complexité de la configuration souhaité. Il est recommandé de bien comprendre les principes de fonctionnement d'un firewall et de vérifier régulièrement les règles de filtrage pour s'assurer que le niveau de sécurité du système est maintenu.

Il est généralement **déconseillé de se connecter directement en tant que root sur un serveur Linux,** car cela peut présenter des risques de sécurité. En effet, si un attaquant réussit à compromettre votre compte root, il aura un accès complet au système et pourra effectuer toutes sortes de modifications, y compris installer des logiciels malveillants ou supprimer des données importantes.

L'utilisation de la commande "sudo" permet de palier ce risque, en permettant à des utilisateurs ordinaires d'exécuter des commandes en tant que root de manière temporaire, avec des privilèges restreints. Cela signifie que les utilisateurs ne peuvent effectuer que des actions autorisées par l'administrateur système.

De plus, en utilisant sudo, il est possible de suivre un journal des actions réalisées avec le compte root, ce qui permet de savoir qui a effectué quelles actions, ce qui est très utile pour le dépannage et l'audit.

En ce qui concerne l'évolution de sudo, **doas est une alternative à sudo** qui est de plus en plus populaire, notamment dans la communauté OpenBSD. Il fait enfin son entrée dans linux.

Doas offre une **syntaxe de configuration plus simple et plus claire** que celle de sudo, ce qui peut faciliter la tâche des administrateurs système. Toutefois, il est important de noter que doas ne possède pas toutes les fonctionnalités de sudo, notamment en ce qui concerne la gestion des règles et des plugins. Par conséquent, il est important de bien évaluer les besoins et les fonctionnalités requises avant de choisir l'un ou l'autre.

Introduction - La sécurité de l'environnement Linux - Exemple d'utilisation de sudo et doas

Pour **exécuter la commande ping en tant que root à partir d'un compte utilisateur normal**, vous pouvez utiliser sudo ou doas.

Voici comment procéder :

Avec sudo :

- Ouvrez un terminal et tapez la commande suivante pour ouvrir le fichier de configuration de sudo : *sudo visudo*
- Ajoutez la ligne suivante à la fin du fichier pour permettre à l'utilisateur de lancer la commande ping en tant que root : *user ALL=(root) NOPASSWD: /bin/ping*
- Remplacez "user" par votre nom d'utilisateur
- Enregistrez le fichier et quittez l'éditeur
- Vous pouvez maintenant exécuter la commande ping en tant que root en tapant :

  sudo ping example.com

Avec doas :

- Ouvrez un terminal et tapez la commande suivante pour ouvrir le fichier de configuration de doas : *doas -u root visudo*
- Ajoutez la ligne suivante à la fin du fichier pour permettre à l'utilisateur de lancer la commande ping en tant que root : *permit user cmd /bin/ping*
- Remplacez "user" par votre nom d'utilisateur.
- Enregistrez le fichier et quittez l'éditeur.
- Vous pouvez maintenant exécuter la commande ping en tant que root en tapant :

  doas ping example.com

Dans les deux cas, vous devriez être en mesure de lancer la commande ping en tant que root à partir de votre compte utilisateur normal.

La différence entre sudo et doas est dans la syntaxe de configuration de leurs fichiers respectifs (sudoers et doas.conf). Dans le cas de doas, la syntaxe est simplifiée et plus facile à lire que celle de sudoers.

SEC-LEC : Durcissement sécurité Linux

Introduction - La sécurité de l'environnement Linux - Liens de données directs

Il est préférable d'interdire l'accès aux ports USB, Firewire et Thunderbolt sur un serveur, car ces ports peuvent être utilisés pour introduire des dispositifs de stockage externes tels que **des clés USB, des disques durs externes ou des appareils mobiles,** qui peuvent être utilisés pour transférer des données sensibles ou malveillantes dans le réseau du serveur. En outre, des périphériques tels que des téléphones mobiles peuvent également être utilisés pour accéder à distance au serveur, ce qui peut présenter des risques de sécurité.

Sous Linux, il existe plusieurs méthodes pour restreindre l'accès aux ports USB, Firewire et Thunderbolt.

Voici deux méthodes courantes :

- Le **fichier de règles Udev** : Udev est un système de gestion de périphériques qui est utilisé dans la plupart des distributions Linux. Le fichier de règles Udev permet de définir des règles qui spécifient les actions à prendre lorsqu'un périphérique est connecté au système. Pour désactiver les ports USB, Firewire et Thunderbolt, il est possible de créer un fichier de règles Udev qui empêche les modules de noyau associés d'être chargés.

  Par exemple, pour désactiver les ports USB, vous pouvez créer un fichier "/etc/udev/rules.d/10-usb.rules" avec le contenu suivant :

  # Disable USB

  install usb-storage /bin/false

- **Des outils de gestion de la sécurité** : De nombreux outils de gestion de la sécurité tels que **AppArmor ou SELinux** peuvent être utilisés pour restreindre l'accès aux ports USB, Firewire et Thunderbolt. Par exemple, avec AppArmor, il est possible de définir des règles qui restreignent l'accès aux ports USB, en utilisant des profils préconfigurés ou en créant des profils personnalisés.

Il est important de noter que la désactivation complète des ports USB, Firewire et Thunderbolt peut avoir des impacts sur la connectivité et la fonctionnalité du système, il est donc recommandé de prendre en compte les besoins spécifiques de votre infrastructure avant de désactiver ces ports.

SEC-LEC : Durcissement sécurité Linux

Introduction - Les tests d'exposition (Shodan)

Shodan est un moteur de recherche spécialisé dans la recherche d'appareils connectés à Internet, tels que des caméras de sécurité, des routeurs, des serveurs, des imprimantes et d'autres types d'appareils connectés à Internet.

Contrairement aux moteurs de recherche traditionnels qui indexent le contenu des pages Web, Shodan indexe les informations sur les appareils connectés à Internet, telles que les ports ouverts, les services en cours d'exécution et les vulnérabilités connues.

Shodan permet aux chercheurs en sécurité, aux professionnels de la sécurité informatique et aux hackers éthiques de rechercher des appareils qui peuvent être vulnérables à des attaques en ligne. Cette information peut être utilisée pour identifier les systèmes qui doivent être corrigés ou mis à jour pour éviter les violations de sécurité.

Les recherches sur Shodan sont effectuées en utilisant des mots clés et des filtres pour affiner les résultats. Les utilisateurs peuvent également afficher des informations telles que les adresses IP, les fournisseurs de services Internet, les noms de domaine et les emplacements géographiques des appareils.

Introduction - Les tests d'exposition (Shodan) - Méthodes d'utilisation

Pour utiliser Shodan, il est nécessaire de se procurer une clé d'API. Pour se faire, nous devons nous enregistrer sur le site shodan.io.

Une fois que l'enregistrement est vérifié, il est possible de se connecter avec votre compte sur le site Shodan.

La clé d'API est disponible dans la partie de gestion du compte de shodan.

Il est recommandé de changer régulièrement la clé d'API pour éviter qu'elle soit trouvée et utilisée par des personnes non-autorisées trop longtemps.

Il est possible de payer pour obtenir plus de services de la part de Shodan : Shodan Billing

Il existe des services similaires à Shodan, comme le français Onyphe ou LeakIX qui autorise les connexions anonymes.

SEC-LEC : Durcissement sécurité Linux

Introduction - Les tests d'exposition (Shodan) - Méthodes d'utilisation

Il y a trois façons distinctes d'utiliser shodan : le site web, la commande shell et la bibliothèque Python :

- **Le site web :**

  Accédez au site web de Shodan à l'adresse shodan.io

  Connectez-vous avec votre compte Shodan ou inscrivez-vous pour en créer un

  Entrez votre requête de recherche dans la barre de recherche, par exemple, "webcam" ou "Apache"

  Utilisez les filtres de recherche pour affiner les résultats selon les critères qui vous intéressent, par exemple, le pays, le type de périphérique, le port ouvert, etc.

  Cliquez sur le bouton "Search" pour afficher les résultats de la recherche

➡ **La commande shell :**

Il faut avoir un python 3 et la librairie pip installée pour continuer.

Installez le client Shodan en exécutant la commande suivante :

pip install shodan

Configurez votre clé API :

shodan init VOTRE_CLÉ_API

Effectuez une recherche :

shodan search apache

Vous pouvez également utiliser des filtres pour affiner les résultats :

shodan search apache country:"FR"

Les détails des commandes utilisables avec la commande se trouvent sur le site Shodan CLI

➡ **La bibliothèque Python :**

Installez la bibliothèque Python de Shodan en utilisant la commande suivante :

pip install shodan

Importez la bibliothèque dans votre script Python :

import shodan

Configurez votre clé API en créant un objet Shodan :

api = shodan.Shodan(YOUR_API_KEY)

Effectuez votre recherche en utilisant la méthode api.search(), par exemple :

resultats = api.search('webcam')

Vous pouvez également utiliser des filtres pour affiner les résultats, par exemple :

resultats = api.search('webcam country:"FR"')

Les détails des fonctions utilisables avec l'API se trouvent sur le site Shodan Python API

SEC-LEC : Durcissement sécurité Linux

Introduction - Les tests d'exposition (Shodan) - Exemple

Demandons à Shodan ce que sa base de données connait des sites publiques de google aux états-unis avec la CLI :

$ pip install shodan

$ shodan

$ shodan init U0DcKIOx5jwL6di1dlBaSttkHxrDHf3p

$ shodan search google.com country=US | cut -d " " -f -2

Il y a un grand nombre résultats, souvent sous amazones.com, pouvez-vous me dire pourquoi ?

SI on refait le test pour microsoft.com, nous allons trouver un résultat équivalent.

Introduction - Outils pour le test d'intrusion - Outils intéressant à connaître

Il existe un grand nombre d'outils destinés à réaliser des tests d'intrusion, j'en présente deux : **hping3** et **hydra**.

hping3 est un outil de test de réseau en ligne de commande utilisé pour envoyer des paquets sur un réseau et analyser les réponses reçues. Il est disponible sur les systèmes d'exploitation Linux, macOS et Windows.

Hping3 peut être utilisé pour diverses tâches, notamment :

- **Détecter les ports ouverts** : Hping3 peut envoyer des paquets TCP, UDP, ICMP ou RAW à une machine distante pour déterminer quels ports sont ouverts et répondent aux requêtes.
- **Évaluer la qualité de service (QoS)** : Hping3 peut envoyer des paquets avec des paramètres spécifiques pour mesurer la latence, la bande passante et d'autres caractéristiques de la connexion réseau.
- **Tester les pare-feux** : Hping3 peut être utilisé pour tester la sécurité d'un pare-feu en envoyant des paquets à différentes fréquences ou avec différents types de données pour déterminer si le pare-feu bloque ou autorise le trafic.
- **Faire du scan de réseau** : Hping3 peut être utilisé pour effectuer un scan de port sur une plage d'adresses IP pour déterminer quels sont les hôtes actifs et quels sont les ports ouverts.

Un appel de base à hping3 : *hping3 -1 localhost*

Introduction - Outils pour le test d'intrusion

hydra est un outil de test de pénétration de réseau en ligne de commande qui est utilisé pour trouver des mots de passe en force brute ou par dictionnaire pour accéder à des systèmes et des services protégés par mot de passe.

L'objectif d'Hydra est de **tester la sécurité des mots de passe** pour divers services tels que les serveurs FTP, les serveurs SSH, les serveurs SMTP, les serveurs POP3, les serveurs HTTP et les services de bases de données, en essayant différentes combinaisons de noms d'utilisateur et de mots de passe.

L'utilisation d'Hydra est assez simple. Il suffit de spécifier le type de service à tester, le nom d'utilisateur, le fichier de mots de passe à utiliser, et éventuellement d'autres options pour personnaliser le test. Hydra exécute ensuite des requêtes automatisées pour tester différentes combinaisons de noms d'utilisateur et de mots de passe jusqu'à ce qu'un mot de passe valide soit trouvé ou que toutes les combinaisons aient été essayées.

Un appel de base à Hydra : *hydra -l formation -p formation localhost ssh*

Des Questions

SEC-LEC : Durcissement sécurité Linux
Le Plan de Sécurité des Systèmes d'Information

SEC-LEC : Durcissement sécurité Linux

Les politiques de sécurité - Définition de Besoin

Les **politiques de sécurité du système d'information (PSSI)** sont importantes pour les organisations car elles permettent de capitaliser sur les expériences passées, les succès et les échecs, pour améliorer la sécurité informatique. Les PSSI sont des documents qui évoluent avec le temps et qui s'adaptent aux nouvelles menaces et aux nouvelles technologies.

Voici quelques exemples des avantages des PSSI :

- **Une base solide pour la sécurité** : Les PSSI permettent de mettre en place une base solide pour la sécurité informatique en définissant les exigences et les procédures nécessaires pour protéger les systèmes d'information contre les cyberattaques et les risques de sécurité.
- **La cohérence et la continuité** : Les PSSI permettent d'assurer la cohérence et la continuité des mesures de sécurité informatique à travers toute l'organisation, même en cas de changement de personnel ou de direction.
- **L'amélioration continue** : Les PSSI permettent d'apprendre de l'expérience en évaluant les mesures de sécurité prises, les résultats obtenus, les échecs et les succès, et en utilisant ces connaissances pour améliorer la sécurité informatique.
- **La conformité réglementaire** : Les PSSI peuvent aider les organisations à se conformer aux lois et réglementations en matière de sécurité informatique en définissant les exigences et les procédures nécessaires pour protéger les données sensibles.
- **La communication et la sensibilisation** : Les PSSI peuvent aider à sensibiliser les employés, les partenaires et les parties prenantes à l'importance de la sécurité informatique, en définissant clairement les rôles et les responsabilités de chacun, ainsi que les mesures de sécurité à suivre.

Les politiques de sécurité - Amélioration Continue

La PSSI est inscrite dans un processus d'amélioration continue.

La Roue de Deming représente l'enchaînement d'évènement conduisant à une amélioration continue.

P : (Plan) Planifie une nouvelle action

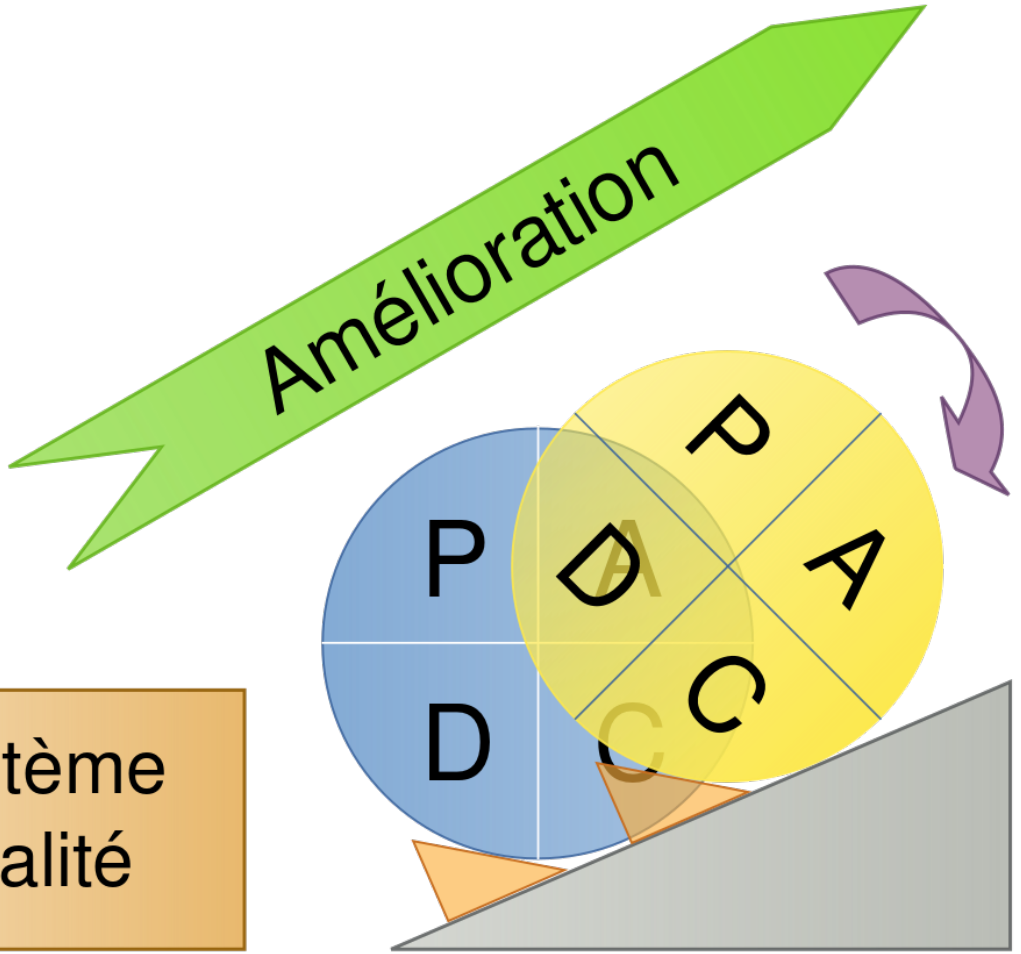
D : (Do) Réalise l'action

C : (Check) Contrôle son efficacité

A : (Act) Réagit en fonction du résultat

L'échec des premiers tests est attendu.

Système qualité



Les politiques de sécurité - Comportement de la PSSI

Une politique de sécurité du système d'information (PSSI) est un document essentiel pour garantir la sécurité informatique d'une organisation.

Voici quelques caractéristiques clés qui doivent être prises en compte lors de la mise en place d'une PSSI :

- **Objectifs clairs** : La PSSI doit définir clairement les objectifs de sécurité à atteindre et les exigences de sécurité qui doivent être respectées.
- **Définition des rôles et des responsabilités** : La PSSI doit établir les rôles et les responsabilités des différents acteurs impliqués dans la sécurité informatique de l'organisation, tels que les administrateurs de systèmes, les utilisateurs et les responsables de la sécurité informatique.
- **Identification des actifs d'information** : La PSSI doit identifier les actifs d'information de l'organisation, tels que les données, les systèmes et les applications, afin de déterminer les risques de sécurité et les mesures de protection nécessaires.
- **Gestion des risques** : La PSSI doit définir une approche structurée pour la gestion des risques, en identifiant les menaces potentielles et en évaluant leur probabilité et leur impact.

Les politiques de sécurité - Comportement de la PSSI

- **Mesures de sécurité** : La PSSI doit énoncer les mesures de sécurité nécessaires pour protéger les actifs d'information, telles que les politiques de gestion des mots de passe, les contrôles d'accès, le cryptage, les sauvegardes et les plans de continuité des activités.
- **Formation et sensibilisation** : La PSSI doit inclure des mesures pour former et sensibiliser les utilisateurs et les employés de l'organisation à l'importance de la sécurité informatique et aux pratiques de sécurité appropriées.
- **Évaluation et audit** : La PSSI doit définir les procédures pour l'évaluation régulière de l'efficacité des mesures de sécurité, ainsi que pour les audits de sécurité informatique.
- **Adaptabilité** : La PSSI doit être adaptable pour prendre en compte les nouvelles menaces et les nouvelles technologies qui peuvent affecter la sécurité informatique de l'organisation.

En somme, une PSSI efficace doit être claire, exhaustive, adaptable et régulièrement révisée et mise à jour pour garantir une protection optimale contre les risques de sécurité informatique.

SEC-LEC : Durcissement sécurité Linux

Les politiques de sécurité - Héritage de la PSSI

Le Plan de Sécurité des Systèmes d'Information (PSSI) est un document élaboré par la maison-mère et doit être respecté par toutes les filiales et sites de l'entreprise.

Cependant, **les besoins en matière de sécurité peuvent varier** d'une filiale à l'autre et d'un site à l'autre, en fonction des réglementations locales, des risques spécifiques et des exigences opérationnelles. Par conséquent, il est souvent nécessaire d'adapter le PSSI de la maison-mère aux besoins locaux des filiales et des sites.

Prenons l'exemple d'une usine de type CEVESO qui doit adapter le PSSI de sa maison-mère aux réglementations qui s'appliquent à son cas particulier. Cette usine travaille avec des matières dangereuses et est soumise à des règles strictes en matière de sécurité. **Elle doit donc adapter le PSSI de sa maison-mère en fonction des réglementations en vigueur dans le pays où se situe l'usine.**

Tout d'abord, l'usine CEVESO doit effectuer **une analyse de risque** pour identifier les menaces et les vulnérabilités spécifiques à son site. Ensuite, elle doit adapter les politiques et les procédures du PSSI d'origine pour répondre à ces risques, tout en respectant les exigences de la maison-mère. Par exemple, l'usine CEVESO pourrait mettre en place **des mesures de sécurité supplémentaires** pour gérer les risques liés aux matières dangereuses, telles que la surveillance en temps réel, l'identification et la gestion des incidents, la formation du personnel, etc.

Enfin, il est important que **l'usine CEVESO assure la communication et la coordination avec la maison-mère** pour s'assurer que les adaptations apportées respectent les demandes et les directives du PSSI d'origine. Cela peut nécessiter des discussions régulières avec la direction de la maison-mère pour s'assurer que les adaptations sont bien comprises et acceptées.

En somme, adapter le PSSI de la maison-mère aux besoins locaux des filiales et des sites est crucial pour assurer une sécurité optimale des systèmes d'information. L'exemple de l'usine CEVESO montre que cela peut impliquer l'analyse des risques, l'adaptation des politiques et procédures, et la communication avec la maison-mère pour assurer la conformité globale avec le PSSI d'origine.

Les politiques de sécurité - Caractéristiques d'une PSSI

Les **politiques de sécurité du système d'information (PSSI)** sont des ensembles de directives et de procédures qui définissent comment une organisation protège ses informations, son réseau et ses systèmes contre les menaces internes et externes. Les PSSI comprennent les mesures de sécurité techniques, organisationnelles et humaines visant à protéger les actifs d'information contre les cybermenaces et les risques de sécurité informatique.

Voici quelques exemples de politiques de sécurité du système d'information :

- **Politique de gestion des mots de passe** : cette politique énonce les exigences relatives à la création et à la gestion des mots de passe pour les comptes d'utilisateurs, les périphériques, les systèmes et les applications. Elle peut inclure des exigences telles que des mots de passe complexes, des politiques de renouvellement de mot de passe, la limitation du nombre de tentatives de connexion et la nécessité de protéger les mots de passe.
- **Politique de contrôle d'accès** : cette politique énonce les exigences relatives à l'accès aux données et aux ressources informatiques, en fonction des autorisations et des privilèges accordés aux utilisateurs. Elle peut inclure des exigences telles que des restrictions sur les horaires d'accès, des autorisations basées sur les rôles et les responsabilités, ainsi que des audits pour surveiller les activités d'accès.

SEC-LEC : Durcissement sécurité Linux

Les politiques de sécurité - Caractéristiques d'une PSSI

- **Politique de chiffrement** : cette politique énonce les exigences relatives à l'utilisation du chiffrement pour protéger les données sensibles contre les accès non autorisés. Elle peut inclure des exigences telles que l'utilisation de chiffrement pour les données stockées ou en transit, des exigences minimales pour les algorithmes de chiffrement, ainsi que des exigences de gestion des clés de chiffrement.
- **Politique de sauvegarde et de récupération** : cette politique énonce les exigences relatives à la sauvegarde et à la récupération des données, des systèmes et des applications en cas de sinistre ou d'incident de sécurité. Elle peut inclure des exigences telles que des stratégies de sauvegarde régulières, des tests de récupération réguliers, ainsi que des exigences pour la conservation des données de sauvegarde.
- **Politique de gestion des vulnérabilités** : cette politique énonce les exigences relatives à la gestion des vulnérabilités, y compris les processus pour l'identification, l'évaluation, la priorisation et le traitement des vulnérabilités. Elle peut inclure des exigences telles que des analyses de vulnérabilité régulières, des correctifs de sécurité réguliers, ainsi que des processus de communication des vulnérabilités aux parties prenantes concernées.

Ces politiques de sécurité du système d'information doivent être mises en place de manière cohérente et rigoureuse pour garantir une sécurité efficace des systèmes informatiques.

SEC-LEC : Durcissement sécurité Linux

Les politiques de sécurité - Caractéristiques d'une PSSI - Disposition

Une **politique de sécurité du système d'information (PSSI)** se décompose en trois documents distincts, afin de mieux organiser et structurer les différentes informations.

Les trois documents sont généralement les suivants :

- **La politique de sécurité informatique** : C'est généralement le document principal de la PSSI, il décrit les objectifs de sécurité et les mesures de protection que l'organisation doit mettre en place pour protéger ses actifs informatiques. Cette politique doit également définir les rôles et les responsabilités de chacun des acteurs de la sécurité informatique, les mesures de sécurité qui doivent être appliquées pour protéger les systèmes et les données, ainsi que les procédures à suivre en cas d'incident de sécurité. C'est le document le plus largement disponible avec le moins de restrictions de sécurité.
- **Les normes de sécurité informatique** : Il est destiné à fournir des détails spécifiques sur les mesures de sécurité qui doivent être mises en place pour atteindre les objectifs de sécurité définis dans la politique de sécurité informatique. Les normes de sécurité informatique peuvent inclure des informations détaillées sur les politiques de gestion des mots de passe, les contrôles d'accès, les sauvegardes et les plans de continuité des activités, ainsi que d'autres mesures de sécurité spécifiques.
- **Les procédures de sécurité informatique** : Il fournit des instructions détaillées sur les procédures à suivre pour mettre en place les mesures de sécurité décrites dans la politique de sécurité informatique et les normes de sécurité informatique. Les procédures de sécurité informatique peuvent inclure des instructions sur la configuration des systèmes, la gestion des accès, la surveillance des activités de sécurité, les tests de vulnérabilité et les audits de sécurité.

Les deux derniers documents ont des capacités de diffusion restreintes car ils contiennent des détails sur l'implémentation du SI qui doivent rester confidentiels.

Plan de Sécurité des systèmes d'Information - Types de politiques de sécurité

Il existe différents types de politiques de sécurité selon les besoins et les objectifs de l'organisation :

- **Politique de sécurité informatique générale** : Cette politique est une politique de sécurité informatique de base qui vise à établir des règles et des procédures de sécurité pour protéger les actifs informatiques de l'organisation. Elle peut inclure des exigences de mots de passe, des règles d'accès, des procédures de sauvegarde et de récupération, et des mesures de sécurité physique.
- **Politique de sécurité réseau** : Cette politique est conçue pour protéger les réseaux de l'organisation contre les menaces externes et internes, en définissant des règles et des procédures de sécurité pour la gestion des réseaux, les pare-feux, la détection d'intrusions et la surveillance des réseaux.
- **Politique de sécurité des applications** : Cette politique est destinée à protéger les applications et les systèmes de l'organisation, en définissant des règles et des procédures de sécurité pour le développement et la gestion des applications. Elle peut inclure des exigences de codage sécurisé, des règles de gestion des accès, des procédures de test et d'évaluation de la sécurité des applications.
- **Politique de sécurité des données** : Cette politique est conçue pour protéger les données de l'organisation, en définissant des règles et des procédures de sécurité pour la gestion des données, le stockage et la protection de la vie privée. Elle peut inclure des exigences de confidentialité, des règles de classification des données, des procédures de gestion de la vie privée, et des mesures de sécurité pour le stockage et la transmission de données.
- **Politique de sécurité de la conformité** : Cette politique est conçue pour garantir que l'organisation respecte les lois et les réglementations en matière de sécurité informatique. Elle peut inclure des exigences pour la protection des données personnelles, la confidentialité des données, la sécurité des transactions électroniques, et des mesures de sécurité pour les secteurs réglementés comme la santé, les finances, etc.

Plan de Sécurité des systèmes d'Information - Normes et standards de sécurité

Les normes et standards de sécurité informatique sont des documents de référence qui définissent les meilleures pratiques et les exigences pour la sécurité informatique.

Voici quelques-unes des normes et standards de sécurité informatique les plus courants :

- **ISO27001** : La norme ISO/IEC 27001 est une norme internationale qui établit les exigences pour un système de gestion de la sécurité de l'information (SMSI). Elle fournit un cadre pour la mise en place, la mise en œuvre, l'exploitation, la surveillance, la révision, la maintenance et l'amélioration continue d'un SMSI.
- **ISO27002** : Cette norme fournit un code de pratique pour la gestion de la sécurité de l'information. Elle établit des lignes directrices et des principes pour la mise en place de mesures de sécurité de l'information dans l'organisation, en se concentrant sur les processus de gestion des risques.
- **NIST SP 800-53** : Cette norme fournit un ensemble de contrôles de sécurité pour protéger les systèmes et les données contre les menaces de sécurité. Elle est souvent utilisée pour la conformité réglementaire dans le secteur public aux États-Unis.
- **PCI DSS** : La norme PCI DSS (Payment Card Industry Data Security Standard) est une norme de sécurité des paiements électroniques qui établit les exigences de sécurité pour les organisations qui traitent des transactions par carte de crédit ou de débit. Elle fournit des exigences pour la sécurité des données des titulaires de cartes, des réseaux, des systèmes et des applications.
- **CIS Controls** : Le Center for Internet Security (CIS) propose un ensemble de 20 contrôles de sécurité qui couvrent les aspects clés de la sécurité informatique. Ces contrôles peuvent être utilisés pour aider les organisations à identifier et à atténuer les risques de sécurité informatique.

SEC-LEC : Durcissement sécurité Linux

Plan de Sécurité des systèmes d'Information - Normes et standards de sécurité

- **Le référentiel général de sécurité (RGS)** est une norme française qui définit les exigences de sécurité pour les systèmes d'information de l'administration publique française. Le RGS a été conçu pour garantir la sécurité des données et des systèmes informatiques utilisés par les administrations publiques.
- **La norme HDS (Hébergeur de Données de Santé)** est une norme française qui définit les exigences de sécurité pour les hébergeurs de données de santé. Les hébergeurs de données de santé doivent être conformes à cette norme pour pouvoir héberger des données de santé en France.
- **La certification SecNumCloud** est une certification française pour les prestataires de services de cloud computing. Cette certification garantit que le prestataire de services de cloud computing respecte les exigences de sécurité définies par l'ANSSI.

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) élabore également des guides et des recommandations pour la sécurité informatique en France. Ces guides couvrent divers aspects de la sécurité informatique, tels que la gestion des identités, la protection des données et la sécurité des réseaux.

Il existe de nombreuses autres normes et standards de sécurité informatique qui peuvent être pertinents en fonction des besoins et des objectifs de l'organisation. Il est important de comprendre que ces normes et standards ne sont pas une solution unique pour la sécurité informatique, mais plutôt des guides pour aider les organisations à identifier et à atténuer les risques de sécurité. Les organisations peuvent choisir d'utiliser ces normes et standards comme point de départ pour la mise en place d'un programme de sécurité informatique efficace.

SEC-LEC : Durcissement sécurité Linux

Plan de Sécurité des systèmes d'Information - Normes et standards de sécurité - Version Militaire

Les normes et réglementations LPM, NIS et IGI1300 sont des règles établies pour garantir la sécurité et la protection des informations sensibles et classifiées en France.

Voici une description plus détaillée de ces normes :

- **LPM (Loi de Programmation Militaire)** : La LPM est une loi française qui définit la politique de défense et de sécurité nationale et les moyens alloués pour une période donnée. Elle concerne notamment les Opérateurs d'Importance Vitale (OIV) et les Opérateurs de Services Essentiels (OSE) qui sont soumis à des obligations de sécurité renforcées. Les OIV et les OSE doivent ainsi mettre en place des mesures de sécurité pour protéger leurs systèmes d'information et les données qu'ils manipulent.
- **NIS (NATO Information Security)** : La NIS est un ensemble de règles et de procédures de sécurité de l'information élaborées par l'OTAN pour protéger les informations classifiées ou sensibles des membres de l'alliance. La NIS est utilisée par les gouvernements des pays membres de l'OTAN pour protéger leurs informations.
- **IGI 1300** : L'IGI 1300 est un guide d'interprétation des règles de sécurité de l'information établi par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en France. Il fournit des recommandations pour la mise en place de mesures de sécurité pour protéger les informations classifiées ou sensibles. Ce guide s'applique aux OIV et OSE, ainsi qu'à tout organisme ou entreprise qui doit protéger des informations sensibles.
- **La future NIS2** est une mise à jour de la NIS actuelle, qui vise à renforcer la sécurité de l'information en Europe. Elle prend en compte les évolutions technologiques et les nouvelles menaces liées à la sécurité de l'information, et fournit des directives plus strictes pour la protection des informations classifiées ou sensibles. La NIS2 s'applique aux OIV et OSE, ainsi qu'à toute entreprise qui fournit des services essentiels et aux autorités publiques. Elle prend effet à partir du 18 octobre 2024 et sera mise en place dans l'ensemble de l'Union européenne.

SEC-LEC : Durcissement sécurité Linux

Plan de Sécurité des systèmes d'Information - Exemple d'écriture de politique de sécurité du système

Dans le cadre d'une PSSI concernant la gestion des mots de passe, étudiez le cas particulier du verrouillage d'un compte linux pour 30 minutes après 3 essais en échec.

On aurait pu parler de :

- **Complexité des mots de passe** : Les mots de passe doivent être suffisamment complexes pour être difficiles à deviner ou à pirater. Ils doivent contenir une combinaison de lettres, de chiffres et de caractères spéciaux
- **Fréquence de renouvellement** : Les utilisateurs doivent être invités à changer leurs mots de passe régulièrement, au moins tous les trois mois
- **Interdiction de l'utilisation de mots de passe courants** : Les utilisateurs doivent être encouragés à ne pas utiliser de mots de passe courants, tels que "123456" ou "motdepasse"
- **Utilisation d'authentification à deux facteurs** : Lorsque cela est possible, les utilisateurs doivent être encouragés à utiliser l'authentification à deux facteurs, qui ajoute une couche supplémentaire de sécurité à la connexion en demandant une seconde forme d'identification, telle qu'un code envoyé par SMS
- **Stockage des mots de passe** : Les mots de passe doivent être stockés de manière sécurisée, par exemple en utilisant un gestionnaire de mots de passe
- **Sensibilisation et formation** : Les utilisateurs doivent être sensibilisés aux risques liés à la gestion des mots de passe et formés à la création de mots de passe forts
- **Politique de verrouillage des comptes** : Si un utilisateur entre un mot de passe incorrect un certain nombre de fois, son compte doit être verrouillé pour empêcher toute tentative de piratage

SEC-LEC : Durcissement sécurité Linux

Plan de Sécurité des systèmes d'Information - Correction de politique de sécurité du système

- **Politique de sécurité (niveau 1)** : La politique de sécurité inclut une section sur la **gestion des comptes utilisateur,** qui définit les règles et les pratiques de sécurité applicables à la création, la modification et la suppression des comptes d'utilisateurs sous Linux. Cette section inclut une **politique de verrouillage des comptes** qui décrit les mesures de sécurité applicables à la protection des comptes d'utilisateurs. Cette politique de verrouillage de compte **doit inclure les paramètres suivants** :
  * Un maximum de 3 tentatives de connexion incorrectes avant le verrouillage du compte utilisateur
  * Une durée de verrouillage de 30 minutes pour les comptes verrouillés
- **Document de procédures de sécurité (niveau 2)** : Le document de procédures de sécurité décrit les mesures de sécurité spécifiques pour la gestion des comptes d'utilisateurs sous Linux. Ce document doit inclure des procédures étape par étape pour la configuration des paramètres de verrouillage de compte, y compris :
  * La configuration du paramètre **MAX_LOGIN_TRIES** dans le fichier de configuration /etc/login.defs à la valeur 3 pour spécifier le nombre maximum de tentatives de connexion incorrectes
  * La configuration du paramètre **LOGIN_RETRIES** dans le fichier de configuration /etc/default/login à la valeur 3 pour spécifier le nombre maximum de tentatives de connexion incorrectes
  * La configuration du paramètre **FAIL_DELAY** dans le fichier de configuration /etc/login.defs à la valeur 1800 pour spécifier la durée de verrouillage du compte en secondes
- **Document d'exploitation et de maintenance (niveau 3)** : Le document d'exploitation et de maintenance décrit les **procédures d'exploitation et de maintenance associées à la gestion des comptes d'utilisateurs**, telles que la surveillance des journaux de connexion, la gestion des alertes de tentative de connexion frauduleuse, la gestion des violations de sécurité et les procédures de récupération de compte. Ce document doit inclure des procédures de suivi du statut des mots de passe et de la disponibilté des comptes

Des Questions

SEC-LEC : Durcissement sécurité Linux

Guide des bonnes pratiques de déploiement du système Linux - Matériel

Lorsque vous déployez un système Linux, il est important de choisir du matériel compatible avec Linux. Il existe de nombreuses distributions Linux, chacune avec ses propres exigences matérielles, donc il est important de vérifier les spécifications recommandées pour la distribution que vous avez choisie.

Voici quelques bonnes pratiques à prendre en compte lors du choix et du déploiement de matériel pour un système Linux :

- **Vérifiez la compatibilité matérielle** : Vérifiez que tous les composants de votre système sont compatibles avec Linux, y compris les processeurs, les cartes mères, les cartes graphiques, les périphériques de stockage et les adaptateurs réseau.
- **Choisissez du matériel fiable** : Il est important de choisir des composants fiables pour éviter les pannes et les interruptions de service. Vérifiez les avis des utilisateurs, les tests de fiabilité et les recommandations de la communauté Linux avant d'acheter du matériel.
- **Utilisez des pilotes Linux** : Vérifiez que les pilotes nécessaires pour votre matériel sont disponibles pour Linux. Vous pouvez vérifier la compatibilité des pilotes sur les sites Web des fabricants ou sur les forums de la communauté Linux.
- **Évitez les composants propriétaires** : Évitez les composants propriétaires autant que possible, car ils peuvent ne pas être compatibles avec Linux ou ne pas être pris en charge par les pilotes Linux.
- **Optimisez les performances** : Si vous avez besoin de performances élevées, vous pouvez choisir des composants haut de gamme pour votre système, tels que des processeurs multi-cœurs, des disques SSD et des cartes graphiques puissantes.
- **Utilisez des outils de surveillance** : Il est important de surveiller les performances de votre matériel pour détecter les problèmes et les pannes avant qu'ils ne deviennent critiques. Des outils de surveillance tels que Centreon, Zabbix ou Grafana peuvent être utilisés pour surveiller la charge du processeur, l'utilisation de la mémoire, l'utilisation du disque et la température du matériel.

En suivant ces bonnes pratiques, vous devriez être en mesure de choisir et de déployer du matériel fiable et compatible avec Linux pour votre système, tout en optimisant les performances et en minimisant les interruptions de service.

SEC-LEC : Durcissement sécurité Linux

Guide des bonnes pratiques de déploiement du système Linux - Matériel - fwupd

A propos de la mise à jour des firmware des ordinateurs sous linux, **firmware update daemon** (fwupd) est un projet open-source développé par Richard Hughes qui permet le suivi et la mise à jour des firmware de périphériques tels que les ordinateurs portables, les cartes mères, les imprimantes, les souris, les claviers, etc.

fwupd permet de mettre à jour le firmware de ces périphériques via une interface graphique conviviale ou une ligne de commande. Il utilise le protocole LVFS (Linux Vendor Firmware Service) pour récupérer les mises à jour de firmware directement depuis les sites web des fabricants, et peut également être utilisé pour mettre à jour les périphériques via des fichiers de micrologiciel locaux.

fwupd est disponible sur la plupart des distributions Linux, notamment Ubuntu, Debian, Fedora, Arch Linux, et est également pris en charge par les principales distributions commerciales comme Red Hat Enterprise Linux, ubuntu et SUSE Linux Enterprise.

L'un des avantages de fwupd est qu'il est facile à utiliser et automatise la mise à jour du firmware des périphériques, ce qui peut aider à résoudre des problèmes de sécurité et de compatibilité. Il fournit également des informations sur les mises à jour de firmware disponibles et les changements qu'elles apportent, ce qui peut aider les utilisateurs à décider s'ils souhaitent ou non mettre à jour leur firmware.

/!\ : Pour fonctionner, fwupd nécessite que UEFI soit activé.

fwupd devrait déjà être installé sur vos systèmes.

On utilise fwupd de cette façon :

Dans le but de faire la liste du matériel reconnu par fwupd :

fwupdmgr get-devices

La sortie de la commande ressemble à ceci :

SEC-LEC : Durcissement sécurité Linux

Guide des bonnes pratiques de déploiement du système Linux - Matériel - fwupd

```
NOT SPECIFIED NOT SPECIFIED
|
├──1100 MTFDDAK256TBN:
|     Device ID:          72ae8120d30d5931388ccba2086bccbd40c49b67
|     Summary:            ATA drive
|     Current version:    M0MU031
|     Vendor:             Micron (ATA:0x1344, OUI:00a075)
|     Serial Number:      170515A79BF9
|     GUIDs:              26df2a0f-a205-59b4-82d9-f65fcc0ab8d5 ← IDE\Micron_1100_MTFDDAK256TBN_____________M0MU031
|                         303c316a-7bce-56ee-9fa4-76de99ef199f ← IDE\0Micron_1100_MTFDDAK256TBN_____________
|                         2b2029d4-e11a-5e21-bc33-2c0aa91a54c0 ← Micron_1100_MTFDDAK256TBN
|     Device Flags:       • Internal device
|                         • Updatable
|                         • System requires external power source
|                         • Needs a reboot after installation
|                         • Device is usable for the duration of the update
|
└──Atom™ CPU C2338 @ 1.74GHz:
      Device ID:          4bde70ba4e39b28f9eab1628f9dd6e6244c03027
      Current version:    0x0000012d
      Vendor:             Intel
      GUIDs:              b9a2dd81-159e-5537-a7db-e7101d164d3f ← cpu
                          30249f37-d140-5d3e-9319-186b1bd5cac3 ← CPUID\PRO_0&FAM_06
                          86681503-da65-5ad5-a945-04108761acd8 ← CPUID\PRO_0&FAM_06&MOD_4D
                          36775a15-c8e6-5f9a-9c86-f634cee44325 ← CPUID\PRO_0&FAM_06&MOD_4D&STP_8
      Device Flags:       • Internal device
```

Guide des bonnes pratiques de déploiement du système Linux - Matériel - fwupd

Nous voulons maintenant rafraîchir la base de données locale des firmware disponibles avec le master distant :

fwupdmgr refresh

La sortie de la commande ressemble à ceci :

Updating lvfs
Downloading... [**]
Downloading... [**]
Downloading... [**]
Successfully downloaded new metadata: 0 local devices supported

Pour vérifier les mises à jours disponibles :

fwupdmgr get-updates

La sortie de la commande ressemble à ceci :

Devices with no available firmware updates:

- *1100 MTFDDAK256TBN*

No updatable devices

Et, finalement, pour appliquer les mises à jours trouvées, s'il y en a :

fwupdmgr update

La sortie de la commande ressemble à ceci :

Devices with no available firmware updates:

- *1100 MTFDDAK256TBN*

No updatable devices

Ou montre les traces de la mise à jour, et potentiellement propose de rebooter quand il vous conviendra.

fwupd dispose aussi d'un outil permettant de faire un tour bas niveau de votre machine afin de vous fournir des indices sur ce que pourrait poser problème.

fwupdtool security

Le résultat s'appelle result.list.

Nous avons une revue de ce qu'il est possible de faire pour sécuriser un serveur à bas niveau :

- Paramétrage du BIOS,
- Secure Boot UEFI,
- Accès TPM2.0
- Différentes fonctionnalité du CPU
- Chiffrement de la RAM
- Chiffrement du swap

SEC-LEC : Durcissement sécurité Linux

Guide des bonnes pratiques de déploiement du système Linux - Démarrage - Bootloader

Après la fin du lancement du bios, il passe la main (sous linux) à une étape intermédiaire appelée boot-loader.

Actuellement, deux outils se disputent la primauté à ce niveau :

- GNU Grand Unified Boot loader (grub) : Permet à l'utilisateur de sélectionner le système d'exploitation ou noyau qui doit être chargé au démarrage du système. Il permet également à l'utilisateur de transmettre des arguments au noyau. C'est le plus ancien et il dispose d'une énorme base installée. Il est littéralement capable de faire tout ce dont vous pouvez rêver, au prix de la complexité de configuration
- systemd-boot : Étant un nouveau venu, il est moins riche en fonctionnalité et se limite aux démarrages sous UEFI. Il évite de ce fait de devoir charger un système complet. Mais, c'est généralement largement suffisant pour les ordinateurs modernes destinés à faire serveurs en datacenter, desktop ou même laptop.

Il existe un outil (spectre-meltdown-checker) qui permet de faire un tour complet des vulnérabilités du CPU de type spectre présente dans vos ordinateurs et des mesures prises par le kernel, au-delà des messages présents dans le journal du boot de l'ordinateur.

Il est présent dans les paquets standard de vos distributions :

sudo apt install spectre-meltdown-checker

On le lance sous la forme :

sudo specter-meltdown-checker

On obtient un long rapport à étudier contenant un grand nombre de paragraphe de ce genre :

```
* Mitigated according to the /sys interface: YES (Mitigation: Clear CPU buffers; SMT disabled)
* Kernel supports using MD_CLEAR mitigation: YES (md_clear found in /proc/cpuinfo)
* Kernel mitigation is enabled and active: YES
* SMT is either mitigated or disabled: YES
> STATUS: NOT VULNERABLE (Your microcode and kernel are both up to date for this mitigation, and mitigation is enabled)
```

SEC-LEC : Durcissement sécurité Linux

Guide des bonnes pratiques de déploiement du système Linux - Configuration du noyau

La sécurité du noyau Linux est essentielle pour assurer la fiabilité et la confidentialité des systèmes d'exploitation qui l'utilisent.

Elle repose sur plusieurs mécanismes, notamment la sélection des modules et le paramétrage des tunables une fois le kernel chargé.

- **La sélection des modules** consiste à choisir les modules à charger dans le noyau pour garantir leur sécurité et leur fiabilité. Les modules sont des composants logiciels qui peuvent être chargés dynamiquement dans le noyau pour ajouter des fonctionnalités. Cependant, ils peuvent également représenter une menace pour la sécurité s'ils sont malveillants ou vulnérables. Pour éviter cela, il est recommandé de charger uniquement les modules nécessaires pour le fonctionnement du système et de désactiver les modules inutiles ou potentiellement dangereux.
- **Le paramétrage des tunables** consiste à configurer les variables de système du noyau pour optimiser la sécurité et la fiabilité du système. Les tunables peuvent être utilisés pour activer ou désactiver certaines fonctionnalités du noyau, pour limiter l'accès à certaines ressources, ou pour renforcer la protection contre les attaques. Les tunables peuvent être configurés via le fichier de configuration du noyau, le fichier /etc/sysctl.conf ou via la commande sysctl.

Il est important de noter que la sécurité du noyau Linux dépend également d'autres facteurs, tels que la configuration du système de fichiers, la gestion des utilisateurs et des permissions, et les politiques de sécurité en place. Par conséquent, il est recommandé de prendre en compte l'ensemble de ces éléments pour renforcer la sécurité du système.

SEC-LEC : Durcissement sécurité Linux

Guide des bonnes pratiques de déploiement du système Linux - Configuration du noyau - Sélection des modules

La sécurité du noyau Linux dépend de plusieurs facteurs, notamment la sélection des modules et fonctionnalités utiles lors de la compilation du noyau.

Voici quelques pratiques qui peuvent aider à renforcer la sécurité du noyau Linux :

- **Minimiser le nombre de modules et fonctionnalités** : Lors de la compilation du noyau, il est important de ne sélectionner que les modules et fonctionnalités nécessaires au système en question. Moins de modules signifie moins de code qui peut potentiellement être exploité. Il est donc important de désactiver les fonctionnalités qui ne sont pas nécessaires pour le système en question.
- **Désactiver les options non sécurisées** : Certaines fonctionnalités peuvent présenter des risques de sécurité pour le système, comme les protocoles de communication non sécurisés. Il est important de désactiver ces options si elles ne sont pas nécessaires.
- **Activer les fonctionnalités de sécurité du noyau** : Le noyau Linux dispose de plusieurs fonctionnalités de sécurité intégrées, telles que la randomisation de l'espace d'adressage, l'exécution interdite (NX) et la prévention des attaques par déni de service distribué (DDoS). Il est important d'activer ces fonctionnalités pour renforcer la sécurité du système.
- **Activer les mécanismes de contrôle d'accès** : Le noyau Linux dispose également de mécanismes de contrôle d'accès qui permettent de limiter les actions des utilisateurs et des programmes sur le système. Il est important d'activer ces mécanismes de contrôle d'accès pour empêcher les attaquants d'accéder aux ressources sensibles.
- **Garder le noyau à jour** : Les développeurs de noyau publient régulièrement des mises à jour pour corriger les vulnérabilités de sécurité. Il est important de garder le noyau à jour en appliquant les mises à jour régulières pour garantir que les vulnérabilités de sécurité connues sont corrigées.

Ces pratiques peuvent aider à renforcer la sécurité du noyau Linux, mais il est important de noter que la sécurité ne peut jamais être garantie à 100 %. Il est donc important de mettre en place une stratégie de sécurité globale pour réduire les risques d'attaques.

SEC-LEC : Durcissement sécurité Linux

Guide des bonnes pratiques de déploiement du système Linux - Configuration du noyau - Sélection des modules

La sécurisation du noyau Linux peut également dépendre des différentes étapes de la vie du noyau.

Voici quelques pratiques pour sélectionner les modules et fonctionnalités utiles aux différentes étapes :

- **Compilation du noyau** : Comme je l'ai mentionné précédemment, il est important de sélectionner uniquement les modules et fonctionnalités nécessaires lors de la compilation du noyau. Cela peut être réalisé en déterminant les besoins du système en termes de matériel et de logiciels, puis en désactivant les options non nécessaires.
- **Démarrage du noyau** : Il est important de limiter les options de démarrage du noyau pour minimiser les vulnérabilités potentielles. Cela peut être réalisé en utilisant des options de démarrage sécurisées, telles que la désactivation du mode de débogage, la restriction des accès en écriture à la mémoire, la désactivation des ports USB, etc.
- **Utilisation du noyau** : Pendant l'utilisation du noyau, il est important de limiter l'accès aux ressources sensibles en utilisant des mécanismes de contrôle d'accès tels que les listes de contrôle d'accès (ACL), les groupes d'utilisateurs et les permissions de fichiers. Il est également important de surveiller l'utilisation du système en utilisant des outils tels que les journaux de système et les outils de surveillance.
- **Mise à jour du noyau** : Les développeurs de noyau publient régulièrement des mises à jour pour corriger les vulnérabilités de sécurité. Il est important de garder le noyau à jour en appliquant les mises à jour régulières pour garantir que les vulnérabilités de sécurité connues sont corrigées.
- **Fin de vie du noyau** : Lorsqu'un noyau atteint la fin de sa vie, il n'est plus pris en charge et ne recevra plus de mises à jour de sécurité. Il est important de planifier le remplacement du noyau et de migrer vers un noyau plus récent et pris en charge pour garantir la sécurité du système.

En résumé, la sécurisation du noyau Linux peut être réalisée en sélectionnant les modules et fonctionnalités utiles à différentes étapes de la vie du noyau, en utilisant des mécanismes de contrôle d'accès et de surveillance, et en gardant le noyau à jour avec les mises à jour de sécurité régulières.

SEC-LEC : Durcissement sécurité Linux

Guide des bonnes pratiques de déploiement du système Linux - Configuration du noyau - Sélection des modules

kconfig-hardened-check est un outil open-source utilisé pour analyser les options de configuration d'un noyau Linux et détecter les options qui pourraient affecter la sécurité du noyau. Cet outil est principalement utilisé pour aider les développeurs et les administrateurs système à configurer les options de sécurité appropriées lors de la compilation d'un noyau.

Kconfig-hardened-check utilise une série de règles de sécurité prédéfinies pour analyser les options de configuration du noyau et détecter les options qui pourraient affecter la sécurité. Ces règles incluent des vérifications telles que la détection des options activant le support de l'exécution de code en mode utilisateur (user-mode helpers), la détection des options qui pourraient permettre des accès non autorisés à la mémoire système ou encore la détection des options qui pourraient permettre la modification du comportement par défaut du noyau.

Kconfig-hardened-check est principalement utilisé par les développeurs du noyau et les administrateurs système pour configurer les options de sécurité appropriées lors de la compilation d'un noyau personnalisé. En détectant les options de configuration qui pourraient affecter la sécurité, cet outil peut aider les utilisateurs à configurer un noyau plus sécurisé pour leur système.

Il convient de noter que Kconfig-hardened-check ne garantit pas une sécurité absolue du noyau, mais il peut aider à détecter les options de configuration qui pourraient affecter la sécurité et ainsi contribuer à la mise en place d'un noyau plus sécurisé.

Voici les étapes pour installer et utiliser kconfig-hardened-check sur un système Linux :

- **Clonage du dépôt Git** : Kconfig-hardened-check est un projet open source hébergé sur GitHub. Pour l'installer, vous devez cloner le dépôt Git sur votre système en exécutant la commande suivante :

  git clone https://github.com/a13xp0p0v/kconfig-hardened-check.git

- **Utilisation de kconfig-hardened-check** : Une fois que vous avez compilé l'outil, vous pouvez l'utiliser pour analyser la configuration du noyau. Pour cela, exécutez la commande suivante :

  ./kconfig-hardened-check/bin/kconfig-hardened-check -c /chemin/vers/la/configuration-du-noyau

Le chemin vers la configuration du noyau peut varier en fonction de la distribution Linux que vous utilisez. Sur la plupart des distributions, la configuration du noyau se trouve dans le répertoire /boot.

Pour trouver le bon fichier, vous pouvez utiliser la commande : *file /boot/**

Et rechercher les lignes avec "Linux make config build file, ASCII text"

Après l'exécution de la commande, l'outil affichera une liste de problèmes potentiels de sécurité dans la configuration du noyau. Vous pouvez examiner chaque élément de la liste et prendre les mesures nécessaires pour corriger les problèmes.

Il est important de noter que les avertissements détectés par kconfig-hardened-check ne sont pas toujours des problèmes de sécurité réels. Il est donc important d'examiner chaque avertissement et de déterminer si une action est nécessaire. En outre, il est recommandé d'utiliser kconfig-hardened-check en combinaison avec d'autres outils de sécurité pour assurer la sécurité complète du noyau.

SEC-LEC : Durcissement sécurité Linux

Guide des bonnes pratiques de déploiement du système Linux - Configuration du noyau

Le Kernel Runtime Integrity Checking (LKRG) est un module de sécurité avancée open source pour le noyau Linux.LKRG a été développé par des chercheurs en sécurité de l'Université de technologie de Vienne. Il est compatible avec les distributions Linux populaires, telles que Ubuntu, Fedora et Debian.

En tant que module kernel, il est conçu pour être chargé dynamiquement dans le noyau, ce qui signifie qu'il peut être activé et désactivé en fonction des besoins du système. LKRG s'intègre directement dans le noyau Linux et est capable de surveiller et de filtrer les appels système, de modifier le comportement de certains systèmes de fichiers, et de détecter et de bloquer les tentatives d'injection de code dans le noyau.

En raison de ses fonctionnalités de sécurité avancées, LKRG est souvent utilisé dans les environnements de sécurité sensibles, tels que les centres de données et les systèmes financiers. Cependant, il est important de noter que LKRG n'est pas une solution complète en soi et qu'il doit être utilisé en conjonction avec d'autres outils et bonnes pratiques de sécurité pour protéger efficacement les systèmes.

Guide des bonnes pratiques de déploiement du système Linux - Configuration du noyau

La recompilation du noyau n'est pas obligatoire. Il est possible de profiter du système de gestion des modules du kernel pour lui dire que l'usage d'un certain nombre de modules du kernel n'est pas désiré.

/!\ : Tout ce qui est noté ici n'est pas a copier-coller aveuglément. Posez-vous la question du besoin et des éventuels effets de bord de chacune des lignes présentées plus bas.

La méthode consiste à mettre un fichier de la forme

/etc/modprobe.d/.conf*

contenant des lignes

install <module à interdire> /bin/false

pour que, même si le module est chargé, il ne fasse rien.

Guide des bonnes pratiques de déploiement du système Linux - Configuration du noyau

- Afin de bloquer les réseaux peu utilisés, on peut mettre proposer : *dccp, sctp, rds, tipc, n-hdlc, ax25, netrom, x25, rose, decnet, econet, af_802154, ipx, appletalk, psnap, p8023, p8022, can, atm*

- *Dans le cas des filesystems plus ou moins orphelins, et absente vos ordinateurs : cramfs, freevxfs, jffs2, hfs, hfsplus, squashfs, udf, cifs, nfs, nfsv3, nfsv4, gfs2*

- Un module de test de video4linux : *vivid*

- Bluetooth : *bluetooth, btusb*

- La webcam : *uvcvidéo*

La deuxième étape consiste à checker le kernel pour voir si potentiellement des paramètres ne pourraient pas être modifiés afin le rendre moins sujet aux problèmes. Un grand nombre de paramètres concernent les détails du fonctionnement de la pile réseau linux, bien qu'elle soit reconnue pour être de grande qualité.

Il existe une triple interface pour ce paramètrage :

- Une temporaire, dans le répertoire virtuel */proc/sys*. Les modifications à cet endroit ne résistent pas au reboot
- Une autre consiste à mettre des fichiers contenant les clés modifiées dans le répertoire */etc/sysctl.d*. Puis d'appeler la commande *sysctl --system*
- La dernière consiste à modifier dans le bootloader les paramètres de ligne de commande associés à l'appel du kernel.

Il est impossible de vous montrer la totalité des tunables du kernel.

La liste présente sur le site de suivi du kernel le montre :

The kernel's command-line parameters

Un exemple : je souhaite interdire IPV6 sur un serveur.

- **Dans grub (*/etc/default/grub*)**: *GRUB_CMDLINE_LINUX_DEFAULT="**ipv6.disable=1** quiet splash"*
- **Dans sysctl** *(/etc/syscvtl.d)*, ajouter un fichier contenant :

  net.ipv6.conf.all.disable_ipv6 = 1

  net.ipv6.conf.default.disable_ipv6 = 1
- Mettre 1 dans ***/proc/sys/****net/ipv6/conf/{default,all}/disable_ipv6* pour tester temporairement

SEC-LEC : Durcissement sécurité Linux

Guide des bonnes pratiques de déploiement du système Linux - Démarrage - Systemd

Systemd (et sa documentation) est un système d'initialisation open-source pour les systèmes d'exploitation basés sur Linux. Il est conçu pour gérer les processus de démarrage et d'arrêt du système, ainsi que pour fournir des fonctionnalités avancées telles que la gestion des services système, la journalisation, le contrôle des cgroup, la gestion de l'alimentation, la gestion des sockets et la configuration du réseau.

Systemd remplace le système d'initialisation traditionnel basé sur les scripts SysVinit, qui était largement utilisé dans les distributions Linux auparavant. Il est conçu pour être plus rapide, plus efficace et plus flexible que SysVinit, en utilisant une approche plus modulaire et en fournissant des fonctionnalités avancées pour la gestion des processus et des ressources système.

Parmi les fonctionnalités de systemd, on peut citer:

- Le **démarrage** parallèle des services : Réduction du temps de démarrage global
- La **gestion de la journalisation système** : Journalisation plus rapide et plus efficace des événements système
- La **gestion des unités de services :** Gestion facilitée des services système
- La **gestion des cgroups :** Gestion de la performance et de la sécurité, par une limitation des ressources utilisées par les processus système
- La **gestion de l'alimentation :** Gestion des paramètres d'alimentation du système, tels que la gestion des batteries et de l'état de veille
- La **configuration du réseau** : Configurer du réseau de manière plus flexible et plus complète que les outils de configuration du réseau traditionnels

Guide des bonnes pratiques de déploiement du système Linux - Démarrage - Systemd

Des commandes utiles au niveau du boot avec système se trouve dans la liste suivante :

➡ Obtenir la chronique des matériels découverts, de leurs parmaétrage et des évènements rencontrés lors du démarrage :

journalctl --list-boots : Donne la liste (avec un ID) des boots disponibles

jounalctl --boot <ID> : Liste les évènements systèmes depuis le boot indiqué

journalctl -b : Le boot actuel

➡ Obtenir la liste des services lancés par le boot de la machine, avec des détails :

systemd-analyze time : Donne les délais de démarrage du système en général

systemd-analyze blame : Trie les services démarrés par leur temps de démarrage

systemd-analyze plot : Produit un graphe svg de l'initialisation des services

SEC-LEC : Durcissement sécurité Linux

Guide des bonnes pratiques de déploiement du système Linux - Paquetages logiciels

Les **paquets logiciels Linux**, également appelés paquets de distribution, sont des archives de fichiers contenant des logiciels, des bibliothèques, des fichiers de configuration et d'autres ressources nécessaires à l'exécution d'une application ou d'un service sur un système d'exploitation Linux. Les paquets sont souvent créés et gérés par les communautés de distributions Linux.

Les paquets logiciels Linux sont généralement distribués sous forme de fichiers avec une extension de nom spécifique à la distribution Linux, par exemple ".deb" pour Debian et Ubuntu, ".rpm" pour Red Hat, et ".pkg.tar.xz" pour Arch Linux. Les gestionnaires de paquets sont des outils logiciels qui permettent de gérer les paquets logiciels sur un système Linux. Ces gestionnaires de paquets permettent de télécharger, vérifier, installer, désinstaller, mettre à jour et rechercher des paquets logiciels.

Les **gestionnaires de paquets** les plus courants sur les distributions Linux sont apt (Debian, Ubuntu), dnf (Fedora, Red Hat), pacman (Arch Linux), et zypper (openSUSE). Les paquets logiciels Linux peuvent être téléchargés depuis les dépôts officiels de la distribution, ainsi que depuis des dépôts tiers, des sites web et d'autres sources. Il est important de veiller à ne télécharger que des paquets logiciels de sources fiables pour éviter d'installer des logiciels malveillants sur votre système.

Guide des bonnes pratiques de déploiement du système Linux - Paquetages logiciels

Lors de la création d'un paquet Debian, il y a plusieurs fichiers qui sont utilisés pour définir les détails de la conception. Voici une brève explication de certains de ces fichiers :

- Le fichier **preinst** : ce fichier contient les instructions qui doivent être exécutées avant l'installation du paquet. Ces instructions peuvent inclure la création d'utilisateurs, l'installation de dépendances, la configuration de fichiers, etc. Le fichier preinst est exécuté avant l'installation du paquet et peut être utilisé pour effectuer des opérations qui ne peuvent pas être effectuées pendant l'installation.
- Le fichier **postinst** : ce fichier contient les instructions qui doivent être exécutées après l'installation du paquet. Ces instructions peuvent inclure la configuration de fichiers, le redémarrage de services, etc. Le fichier postinst est exécuté après l'installation du paquet et peut être utilisé pour effectuer des opérations qui ne peuvent pas être effectuées pendant l'installation.
- Le fichier **prerm** : ce fichier contient les instructions qui doivent être exécutées avant la suppression du paquet. Ces instructions peuvent inclure l'arrêt de services, la suppression de fichiers de configuration, etc. Le fichier prerm est exécuté avant la suppression du paquet et peut être utilisé pour effectuer des opérations qui ne peuvent pas être effectuées pendant la suppression.
- Le fichier **postrm** : ce fichier contient les instructions qui doivent être exécutées après la suppression du paquet. Ces instructions peuvent inclure la suppression de fichiers, la suppression d'utilisateurs, etc. Le fichier postrm est exécuté après la suppression du paquet et peut être utilisé pour effectuer des opérations qui ne peuvent pas être effectuées pendant la suppression.

Ces fichiers sont souvent inclus dans le répertoire debian du code source du paquet et peuvent être créés manuellement ou à l'aide d'outils tels que dh_make ou debhelper.

Guide des bonnes pratiques de déploiement du système Linux - Paquetages logiciels

Le répertoire /etc est un répertoire important pour la gestion des paquets dans Debian et ses dérivés. Ce répertoire est utilisé pour stocker les fichiers de configuration de nombreux programmes et services installés sur le système.

Lors de l'installation d'un paquet Debian, les fichiers de configuration associés au paquet sont généralement installés dans le répertoire /etc. Ces fichiers peuvent inclure des fichiers de configuration pour les démons du système, les services, les applications, les bibliothèques et les modules.

Les fichiers de configuration installés dans le répertoire /etc peuvent être modifiés par l'administrateur système pour personnaliser le comportement des applications et des services installés. Cependant, si l'administrateur modifie un fichier de configuration installé par un paquet, cette modification sera écrasée lors de la mise à jour du paquet.

Pour éviter ce problème, les paquets Debian peuvent fournir des scripts de maintenance tels que preinst, postinst, prerm et postrm pour gérer les fichiers de configuration lors de l'installation, de la mise à jour ou de la suppression d'un paquet. Ces scripts peuvent effectuer des sauvegardes des fichiers de configuration existants, fusionner les fichiers de configuration avec les nouveaux fichiers fournis par le paquet, ou demander à l'utilisateur de prendre une décision avant de remplacer les fichiers de configuration existants.

En résumé, le répertoire /etc est un répertoire important pour la gestion des paquets Debian et doit être géré avec soin pour éviter des problèmes de configuration lors des mises à jour de paquets. Les scripts de maintenance peuvent être utilisés pour aider à gérer les fichiers de configuration associés à un paquet et permettre à l'administrateur de personnaliser les fichiers de configuration tout en conservant les modifications lors des mises à jour.

Guide des bonnes pratiques de déploiement du système Linux - Paquetages logiciels

apt-cacher-ng est un serveur de cache de paquets Debian qui permet de stocker localement les paquets Debian téléchargés à partir d'un ou plusieurs dépôts Debian. Il permet aux machines clientes d'utiliser les paquets préalablement téléchargés depuis le serveur de cache local, plutôt que de les télécharger à nouveau depuis les dépôts Debian officiels. Cela peut améliorer considérablement les temps de téléchargement et réduire la consommation de bande passante.

L'utilisation d'un serveur de cache de paquets tel que apt-cacher-ng peut également contribuer à la sécurité d'un système Linux en réduisant la surface d'attaque potentielle. En effet, en utilisant un serveur de cache local, les paquets ne sont téléchargés qu'une seule fois depuis les dépôts Debian officiels, et sont ensuite stockés localement. Cela réduit le nombre de connexions réseau sortantes du système, ce qui peut aider à réduire la surface d'attaque potentielle.

De plus, apt-cacher-ng permet de vérifier l'intégrité des paquets avant leur téléchargement, en utilisant les clés publiques du dépôt. Cela peut contribuer à la sécurité en garantissant que les paquets téléchargés sont authentiques et n'ont pas été altérés en transit.

Enfin, apt-cacher-ng peut également être utilisé pour limiter l'accès aux paquets Debian à un ensemble restreint de machines, ce qui peut aider à renforcer la sécurité en réduisant la surface d'attaque potentielle.

En résumé, l'utilisation de apt-cacher-ng peut contribuer à la sécurité d'un système Linux en réduisant la surface d'attaque potentielle, en garantissant l'intégrité des paquets téléchargés et en limitant l'accès aux paquets Debian à un ensemble restreint de machines.

Guide des bonnes pratiques de déploiement du système Linux - Paquetages logiciels

Voici les étapes de base pour installer et utiliser apt-cacher-ng :

- Installation de apt-cacher-ng : *sudo apt-get install apt-cacher-ng*
- Configuration de apt-cacher-ng : *sudo vi /etc/apt-cacher-ng/acng.conf*
- Décommenter la *ligne # Port:3142* pour permettre à apt-cacher-ng d'écouter sur le port 3142. Vous pouvez également modifier d'autres paramètres de configuration selon vos besoins.
- Démarrage de apt-cacher-ng :*sudo service apt-cacher-ng start*
- Configuration des clients pour utiliser apt-cacher-ng : *sudo nano /etc/apt/apt.conf*
- Ajouter la ligne suivante au fichier de configuration : *Acquire::http::Proxy "http://adresse_IP_du_serveur:3142";*, en remplaçant adresse_IP_du_serveur par l'adresse IP du serveur où apt-cacher-ng est installé.

Une fois ces étapes terminées, apt-cacher-ng est configuré et prêt à être utilisé. Les clients configurés pour utiliser apt-cacher-ng téléchargeront désormais les paquets Debian à partir du serveur de cache local plutôt que des dépôts Debian officiels, ce qui peut améliorer considérablement les temps de téléchargement et réduire la consommation de bande passante.

Notez que si vous utilisez un pare-feu sur votre serveur, vous devrez peut-être autoriser les connexions entrantes sur le port 3142 pour permettre aux clients d'accéder à apt-cacher-ng.

SEC-LEC : Durcissement sécurité Linux

Guide des bonnes pratiques de déploiement du système Linux - Paquetages logiciels

La **recompilation des paquets** dans un but de sécurité est une pratique courante pour les distributions Linux. Cette pratique consiste à recompiler un paquet Debian à partir de ses sources pour inclure des correctifs de sécurité ou des modifications spécifiques pour répondre à des exigences de sécurité particulières.

Il existe plusieurs raisons pour lesquelles la recompilation des paquets peut améliorer la sécurité d'un système Linux. En voici quelques-unes :

- **Vérification de contenu** : Validation de la correspondance entre le contenu binaire du paquet et la description contenue dans les fichiers sources
- **Correction des vulnérabilités connues** : Inclusion des correctifs pour des vulnérabilités connues qui ont été identifiées depuis la version précédente
- **Ajout de mesures de sécurité supplémentaires** : Ajout de mesures de sécurité supplémentaires, telles que la compilation avec des options de sécurité plus strictes ou l'ajout de modules de sécurité supplémentaires
- **Personnalisation pour répondre à des exigences de sécurité spécifiques** : Personnalisation d'un paquet pour répondre à des exigences de sécurité spécifiques, telles que l'utilisation de bibliothèques ou de configurations particulières

Guide des bonnes pratiques de déploiement du système Linux - Paquetages logiciels

La recompilation des paquets peut être réalisée en suivant les étapes suivantes :

- **Récupération des sources du paquet** : Les sources d'un paquet Debian peuvent être récupérées à l'aide de la commande *apt-get source nom_du_paquet*, en remplaçant "nom_du_paquet" par le nom du paquet à recompiler
- **Application des correctifs de sécurité** : Si des correctifs de sécurité sont nécessaires, ils peuvent être appliqués aux sources récupérées à l'étape précédente. Les correctifs peuvent être obtenus à partir de sources en amont ou développés en interne
- **Compilation des sources** : Les sources modifiées doivent être compilées à l'aide des outils de compilation standard, tels que make, gcc ou cmake. Il est important de s'assurer que les options de compilation sont correctement configurées pour inclure les correctifs de sécurité et les mesures de sécurité supplémentaires
- **Création du paquet Debian** : Une fois la compilation terminée, le paquet Debian doit être créé à l'aide de la commande *dpkg-buildpackage*. Ce processus crée un paquet Debian à partir des fichiers binaires et des scripts d'installation générés lors de la compilation
- **Installation du paquet Debian recompilé** : Le paquet Debian recompilé peut maintenant être installé sur le système cible à l'aide de la commande *dpkg -i nom_du_paquet.deb*, en remplaçant "nom_du_paquet.deb" par le nom du fichier du paquet Debian recompilé

Il est important de noter que **la recompilation des paquets peut être une tâche complexe et chronophage**, en particulier pour les paquets complexes ou les environnements où plusieurs dépendances sont requises. Il est également important de s'assurer que les correctifs de sécurité appliqués sont fiables et n'introduisent pas de nouveaux problèmes de sécurité. Par conséquent, il est recommandé de faire appel à des experts en sécurité pour effectuer cette tâche si vous n'avez pas l'expertise nécessaire.

Guide des bonnes pratiques de déploiement du système Linux - Paquetages logiciels

Snap et Flatpak sont deux systèmes de gestion de paquets qui permettent aux développeurs de créer et de distribuer des applications Linux avec toutes leurs dépendances incluses. Ils ont été créés pour résoudre les problèmes de compatibilité entre distributions Linux et pour faciliter l'installation et la mise à jour d'applications sur différents systèmes.

Les deux systèmes ont des fonctionnalités similaires, mais ils diffèrent dans leur approche de certains aspects clés de la gestion de paquets.

Voici une description parallèle de Snap et Flatpak :

➡ **Distribution des paquets :**

Snap utilise son propre système de distribution pour les paquets, qui est géré par Canonical, la société qui développe Ubuntu. Les paquets Snap sont stockés sur des serveurs dédiés appelés "Snap Store". Les développeurs peuvent publier des paquets Snap sur le Snap Store, mais ils doivent respecter les politiques de sécurité et de confidentialité de Canonical.

Flatpak utilise un système de distribution décentralisé, où les paquets sont hébergés sur les serveurs des développeurs. Les paquets peuvent être publiés sur différents référentiels, tels que Flathub, qui est un référentiel de paquets Flatpak populaire.

➡ **Sandboxing** :

Snap et Flatpak utilisent tous deux des technologies de sandboxing pour isoler les applications du système hôte et assurer leur sécurité. Snap utilise AppArmor, qui est un système de confinement de processus, tandis que Flatpak utilise Bubblewrap, qui est une technologie de confinement de processus similaire.

Guide des bonnes pratiques de déploiement du système Linux - Paquetages logiciels

➡ **Compatibilité des distributions :**

Snap est conçu pour être compatible avec différentes distributions Linux, bien qu'il ait été initialement développé pour Ubuntu. Il est censé fonctionner sur la plupart des distributions Linux modernes, y compris Debian, Fedora, Arch Linux, etc.

Flatpak est également conçu pour être compatible avec différentes distributions Linux, mais il est généralement considéré comme étant plus compatible que Snap, car il utilise des bibliothèques communes partagées par les distributions. Cela signifie qu'un paquet Flatpak peut être exécuté sur différentes distributions sans avoir besoin de dépendances spécifiques à la distribution.

➡ **Taille des paquets :**

Les paquets Snap ont tendance à être plus volumineux que les paquets Flatpak, car Snap inclut toutes les dépendances et les bibliothèques nécessaires pour exécuter l'application. Cela peut entraîner une consommation de stockage plus importante.

Flatpak utilise un système de partage de bibliothèques pour éviter la duplication des dépendances, ce qui permet des paquets plus petits et une consommation de stockage moindre.

➡ **Personnalisation des paquets :**

Snap offre une plus grande flexibilité pour la personnalisation des paquets, car les développeurs peuvent inclure des bibliothèques et des dépendances spécifiques à leur application. Cela peut être utile pour les applications qui ont des exigences particulières.

Flatpak utilise une approche plus standardisée, où les applications partagent les mêmes bibliothèques. Cela peut être plus pratique pour les utilisateurs finaux, mais peut limiter les possibilités de personnalisation pour les développeurs.

Guide des bonnes pratiques de déploiement du système Linux - Paquetages logiciels

Voici quelques raisons pour lesquelles vous pourriez envisager de supprimer Snap et Flatpak de votre serveur :

- **Réduction de la surface d'attaque** : Snap et Flatpak sont des systèmes de gestion de paquets qui incluent un moteur d'exécution de sandboxing pour exécuter des applications. Bien que cela puisse améliorer la sécurité, cela peut également introduire de nouvelles vulnérabilités potentielles. En supprimant Snap et Flatpak, vous pouvez réduire la surface d'attaque du système.
- **Simplification de la gestion des paquets** : Si vous n'avez pas besoin de fonctionnalités supplémentaires ou d'applications disponibles uniquement sous Snap ou Flatpak, il peut être plus simple de ne pas les utiliser. En éliminant ces systèmes, vous pouvez simplifier la gestion des paquets et éviter les éventuelles incompatibilités avec les autres paquets.
- **Optimisation des performances** : Snap et Flatpak peuvent nécessiter plus de ressources système que les paquets Debian standard en raison de l'utilisation de moteurs d'exécution sandboxing. Si la performance est une priorité, il peut être préférable de supprimer Snap et Flatpak.

Si vous décidez de supprimer Snap et Flatpak de votre serveur, vous pouvez le faire en utilisant les commandes de gestion de paquets standard telles que apt-get remove snapd et apt-get remove flatpak.

Il est important de noter que la suppression de Snap ou Flatpak peut entraîner la suppression d'applications qui ont été installées à l'aide de ces systèmes de gestion de paquets. Il est donc recommandé de vérifier les applications installées et de les réinstaller si nécessaire après la suppression de Snap ou Flatpak.

SEC-LEC : Durcissement sécurité Linux

Guide des bonnes pratiques de déploiement du système Linux - Partitionnement des disques durs

Le **partitionnement des disques dur**s sous Linux est une étape importante lors de l'installation d'un système d'exploitation Linux ou lors de la configuration d'un serveur Linux. Le partitionnement consiste à diviser le disque dur en plusieurs partitions logiques, chacune ayant son propre système de fichiers et ses propres options de montage. Le partitionnement des disques durs peut être effectué manuellement ou automatiquement lors de l'installation du système d'exploitation.

Voici quelques points clés à prendre en compte lors du partitionnement des disques durs sous Linux :

- **Partition système EFI** : Nécessaire pour démarrer le système d'exploitation en utilisant l'interface UEFI. Elle doit être créée en premier sur le disque dur et doit être formatée avec le système de fichiers FAT32. La taille recommandée pour cette partition est d'au moins 200 Mo.
- **La partition de démarrage (/boot)** : Utilisée sur les systèmes d'exploitation Linux pour stocker les fichiers de démarrage du système. Elle contient les fichiers nécessaires pour démarrer le système d'exploitation, tels que le chargeur de démarrage, les fichiers de configuration du noyau Linux et les images du noyau. La partition /boot doit être suffisamment grande pour stocker les fichiers de démarrage du système, mais elle ne doit pas être trop grande, car cela peut gaspiller de l'espace disque.
- **Partition système (/)** : Contient les fichiers de base du système d'exploitation, tels que le noyau Linux, les programmes d'initialisation et les fichiers de configuration. La taille recommandée pour cette partition est d'au moins 20 Go pour les installations de bureau et de 10 Go pour les serveurs.
- **Partition de swap (/swap)** : La partition de swap est utilisée comme espace de stockage temporaire pour les données qui ne rentrent pas dans la mémoire vive (RAM) du système. La taille de la partition de swap dépend de la quantité de RAM installée sur le système. Elle doit être d'au moins la taille de la RAM, et jusqu'à deux fois la taille de la RAM pour les systèmes à faible mémoire vive.
- **Partition de données (/home)** : La partition de données est l'endroit où les fichiers de l'utilisateur sont stockés. Elle doit être suffisamment grande pour stocker les données utilisateur, les fichiers de configuration, les fichiers de journalisation et les sauvegardes. La taille de cette partition dépend de l'utilisation prévue du système, mais elle peut être augmentée à tout moment si nécessaire.
- **Le système de fichiers** : Le choix du système de fichiers dépend de l'utilisation prévue du système et des exigences de performance. Les systèmes de fichiers les plus couramment utilisés sous Linux sont ext4, XFS et Btrfs. Ext4 est le système de fichiers par défaut pour de nombreuses distributions Linux.
- **Les options de montage** : Les options de montage définissent la façon dont la partition est montée lors du démarrage du système. Les options de montage courantes incluent les options de lecture et d'écriture, les options de sécurité, les options de compression et les options de journalisation.

Il est important de noter que le partitionnement des disques durs peut varier en fonction de l'utilisation prévue du système et des exigences spécifiques de chaque installation. Il est recommandé de bien comprendre les différents types de partitions et les options de montage avant de partitionner les disques durs sous Linux.

Guide des bonnes pratiques de déploiement du système Linux - Partitionnement des disques durs

Un exemple de partitionnement de disque dur :

```
$ sudo parted /dev/sda
GNU Parted 3.5
Using /dev/sda
Welcome to GNU Parted! Type 'help' to view a list of commands.
(parted) unit GB
(parted) print
Model: ATA Micron_1100_MTFD (scsi)
Disk /dev/sda: 256GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:

Number  Start   End     Size    Type     File system     Flags
 1      0.00GB  0.52GB  0.52GB  primary  ext4            boot
 2      0.52GB  255GB   254GB   primary  ext4
 3      255GB   256GB   1.10GB  primary  linux-swap(v1)  swap

(parted) quit
:~$
```

Il est fini le temps où /etc/init.d était le répertoire où les scripts shell se battaient pour faire démarrer les services nécessaires à la bonne marche d'un serveur.

Si vous devez écrire des script shell, pensez à les faire valider par shellcheck. Pas à distance sur leur site, mais à l'aide du paquet de votre distribution.

Exemple : le script install de ronggang/transmission-web-control

- Télécharger le fichier :

  wget https://raw.githubusercontent.com/ronggang/transmission-web-control/master/release/install-tr-control.sh

- Installation de shellcheck :

  sudo apt install spellcheck

- Lancer shellcheck sur install-tr-control.sh :

```
In install-tr-control.sh line 500:
    if [ $? -eq 0 ]; then
            ^-- SC2181 (style): Check exit code directly with e.g. 'if mycmd;', not indirectly with $?.
```

systemd a repris tout ça et a transformé les scripts shell en fichiers de commandes.

SEC-LEC : Durcissement sécurité Linux

Guide des bonnes pratiques de déploiement du système Linux - Les scripts de démarrage

Systemd est un système d'initialisation pour les systèmes d'exploitation Linux. Il est devenu le système d'initialisation standard pour de nombreuses distributions Linux, remplaçant les systèmes d'initialisation plus anciens tels que SysV init.

L'un des aspects les plus importants de systemd est sa capacité à gérer les services, qui sont des programmes qui s'exécutent en arrière-plan pour effectuer des tâches spécifiques sur un système. Les services systemd sont configurés via des fichiers de service, qui spécifient les dépendances du service, le chemin de l'exécutable, les arguments de ligne de commande, les variables d'environnement, etc.

Voici quelques-uns des services les plus couramment utilisés avec systemd :

- **systemd-logind** : service de gestion de la session utilisateur, permettant aux utilisateurs de se connecter, de se déconnecter et de gérer les sessions de manière sécurisée.
- **systemd-journald** : service de gestion des journaux système, qui stocke les informations de journalisation pour le système et les services qui s'exécutent sur celui-ci.
- **systemd-networkd** : service de gestion du réseau, qui configure les interfaces réseau et gère les connexions réseau.
- **systemd-resolved** : service de résolution de noms, qui fournit une résolution de noms local et DNS.
- **systemd-timedated** : service de gestion de la date et de l'heure, qui maintient l'heure du système et peut être utilisé pour synchroniser l'heure du système avec un serveur NTP.

En plus de ces services, systemd fournit également un certain nombre d'autres fonctionnalités, telles que la gestion des contrôleurs de périphériques, la surveillance des processus, la gestion de l'alimentation et de la veille, et bien plus encore. En résumé, systemd est un système d'initialisation puissant et complet qui offre un large éventail de fonctionnalités pour la gestion des systèmes Linux modernes.

SEC-LEC : Durcissement sécurité Linux

Guide des bonnes pratiques de déploiement du système Linux - Les scripts de démarrage

```
$ cat  /etc/systemd/system/syslog.service
[Unit]
Description=System Logging Service                  brève description du service
Requires=syslog.socket                               la présence obligatoire d'une socket de journalisation syslog pour fonctionner
Documentation=man:rsyslogd(8)                        page du manuel qui contient la documentation pour le démon de journalisation Rsyslogd
Documentation=man:rsyslog.conf(5)                    page du manuel qui contient la documentation pour le fichier de configuration de Rsyslog
Documentation=https://www.rsyslog.com/doc/           lien vers la documentation en ligne de Rsyslog

[Service]
Type=notify                                          le service utilise la notification pour signaler qu'il est prêt à recevoir des connexions
ExecStart=/usr/sbin/rsyslogd -n -iNONE               la commande qui est exécutée pour démarrer le démon Rsyslog
StandardOutput=null                                  la sortie standard est redirigée vers /dev/null, donc ignorée
Restart=on-failure                                   le service doit être redémarré automatiquement en cas d'échec

# Increase the default a bit in order to allow many simultaneous
# files to be monitored, we might need a lot of fds.
LimitNOFILE=16384                                    la limite du nombre de fichiers que le service peut ouvrir est augmentée à 16384, ce qui
                                                     peut être utile pour surveiller de nombreux fichiers simultanément

[Install]
WantedBy=multi-user.target                           le niveau d'exécution (runlevel) dans lequel le service doit être lancé. Dans ce cas, le
                                                     service est lancé dans le niveau multi-utilisateur (multi-user.target)

Alias=syslog.service                                 Cette ligne crée un alias pour le service, qui peut être utilisé pour référencer le service
par
                                                     un nom alternatif, dans ce cas "syslog.service"
```

SEC-LEC : Durcissement sécurité Linux

Guide des bonnes pratiques de déploiement du système Linux - Les scripts de démarrage

La commande *systemd-analyze security* permet d'avoir une vision globale du niveau de sécurité de tous les services de votre ordinateur :

```
$ systemd-analyze security
UNIT                                  EXPOSURE PREDICATE HAPPY
ModemManager.service                       6.3 MEDIUM    😐
accounts-daemon.service                    5.5 MEDIUM    😐
cron.service                               9.6 UNSAFE    😨
dbus.service                               9.5 UNSAFE    😨
dmesg.service                              9.4 UNSAFE    😨
emergency.service                          9.5 UNSAFE    😨
freshrss.service                           9.2 UNSAFE    😨
getty@tty1.service                         9.6 UNSAFE    😨
```

...

La commande *systemd-analyze security syslog.service* permet d'avoir une analyse ligne à ligne de la sécurité du service :

```
$ systemd-analyze security syslog
  NAME                                                    DESCRIPTION                                                    EXPOSURE
✗ RootDirectory=/RootImage=                               Service runs within the host's root directory                       0.1
  SupplementaryGroups=                                    Service runs as root, option does not matter
  RemoveIPC=                                              Service runs as root, option does not apply
✗ User=/DynamicUser=                                      Service runs as root user                                           0.4
✗ CapabilityBoundingSet=~CAP_SYS_TIME                     Service processes may change the system clock                       0.2
✗ NoNewPrivileges=                                        Service processes may acquire new privileges                        0.2
✓ AmbientCapabilities=                                    Service process does not receive ambient capabilities
✗ PrivateDevices=                                         Service potentially has access to hardware devices                  0.2
✗ ProtectClock=                                           Service may write to the hardware clock or system clock             0.2
```

...

Le fichier capabilities(7) - Linux manual page regroupe une description de toutes les capabilities disponibles pour chacun des services de systemd.

Guide des bonnes pratiques de déploiement du système Linux - Les scripts de démarrage

En plus des fichiers de service systemd avec l'extension ".service", systemd utilise également d'autres types de fichiers pour gérer différents aspects du système.

Voici quelques exemples :

- **Les fichiers de montages ("mount units")** : ces fichiers, portant l'extension ".mount", sont utilisés pour décrire des points de montage de systèmes de fichiers. Ils peuvent être utilisés pour monter des partitions de disque dur, des partages réseau, etc.
- **Les fichiers de socket ("socket units")** : ces fichiers, portant l'extension ".socket", sont utilisés pour configurer des sockets réseau ou des fichiers UNIX pour accepter des connexions. Les fichiers de service peuvent dépendre de ces sockets pour démarrer ou s'arrêter.
- **Les fichiers de périphériques ("device units")** : ces fichiers, portant l'extension ".device", sont utilisés pour décrire des périphériques matériel ou virtuels. Ils peuvent être utilisés pour effectuer des actions lorsqu'un périphérique est connecté ou déconnecté.
- **Les fichiers de cible ("target units")** : ces fichiers, portant l'extension ".target", sont utilisés pour décrire un ensemble de services à lancer en même temps. Les cibles sont utilisées pour gérer le démarrage et l'arrêt de groupes de services.
- **Les fichiers d'automount ("automount units")** : ces fichiers, portant l'extension ".automount", sont utilisés pour configurer le montage automatique de systèmes de fichiers. Ils sont souvent utilisés pour monter des systèmes de fichiers réseau de manière transparente.
- **Les fichiers de portée ("scope units")** : ces fichiers, portant l'extension ".scope", sont utilisés pour gérer des processus externes à systemd, en surveillant leur utilisation de ressources (mémoire, CPU, etc.). Les portées sont créées automatiquement lorsqu'un processus est lancé à l'aide de systemd-run.

En utilisant ces différents types de fichiers, systemd offre une grande flexibilité pour gérer différents aspects du système. Les fichiers de service restent toutefois les plus couramment utilisés, car ils permettent de configurer le démarrage et l'arrêt de la plupart des services du système.

SEC-LEC : Durcissement sécurité Linux

Guide des bonnes pratiques de déploiement du système Linux - Les scripts de démarrage

La plupart des serveurs Linux n'incluent pas **d'interface graphique (GUI)** telle que Xorg ou Wayland, car ils sont souvent gérés à distance via des connexions SSH ou des interfaces de ligne de commande.

Dans certains cas, l'installation d'une interface graphique sur un serveur Linux peut toutefois être justifiée, par exemple pour exécuter des applications graphiques, pour la configuration du serveur via une interface graphique, ou pour fournir une interface utilisateur à un groupe d'utilisateurs qui préfèrent une interface graphique plutôt qu'une interface de ligne de commande.

Cependant, il est important de noter que l'installation d'une interface graphique peut également introduire des vulnérabilités de sécurité supplémentaires sur le serveur, car les interfaces graphiques ont souvent plus de surface d'attaque que les interfaces en ligne de commande.

Par conséquent, l'installation d'une interface graphique sur un serveur Linux doit être considérée avec prudence, et il est recommandé de suivre les bonnes pratiques de sécurité pour minimiser les risques de sécurité.

Guide des bonnes pratiques de déploiement du système Linux - Réseau

Netplan est un outil de configuration réseau utilisé par les systèmes d'exploitation Linux modernes pour configurer les interfaces réseau. Il remplace l'outil de configuration réseau traditionnel ifupdown, qui est devenu obsolète.

Netplan permet de définir la configuration du réseau de manière claire et simple en utilisant un format YAML, ce qui le rend facile à lire et à comprendre. Il prend en charge les configurations IP statiques, DHCP et les ponts réseau, et peut être utilisé pour configurer des adresses IPv4 et IPv6.

Lorsque la configuration du réseau est modifiée via Netplan, il génère les fichiers de configuration réseau nécessaires pour que les changements prennent effet. Cela peut inclure des fichiers tels que /etc/network/interfaces, /etc/resolv.conf et /etc/hosts.

Netplan est compatible avec de nombreuses distributions Linux, y compris Ubuntu, Debian et Fedora. Il peut être utilisé en ligne de commande ou via une interface graphique, et peut également être intégré à des outils de gestion de configuration tels que Ansible ou Puppet.

En résumé, Netplan est un outil de configuration réseau moderne et facile à utiliser pour les systèmes d'exploitation Linux.

Une exemple simple de fichier de configuration yaml netplan :

```
:~/$ cat /etc/netplan/01-netcfg.yaml
# This file describes the network interfaces available on your system
# For more information, see netplan(5).
network:
  version: 2
  renderer: networkd
  ethernets:
    enp1s0:
      dhcp4: yes
      dhcp6: yes
```

Le paquet iproute2 est un ensemble d'outils pour la gestion et la configuration avancée des interfaces réseau sous Linux. Il est installé par défaut dans de nombreuses distributions Linux, y compris Ubuntu, Debian et CentOS.

Les outils les plus couramment utilisés sont :

- **ip** : un outil polyvalent pour la gestion des adresses IP, des routes, des interfaces réseau, des règles de pare-feu et d'autres aspects de la configuration réseau
- **ss** : Afficher des statistiques de connexion TCP/UDP, des sockets réseau et des informations sur les connexions actives
- **tc** : Configurer et gérer les files d'attente de paquets, les classes de trafic et les règles de QoS (Quality of Service) sur les interfaces réseau
- **arp** : Afficher et modifier la table ARP, qui lie les adresses MAC et IP sur un réseau local
- **bridge** : Créer et manipuler des switch virtuels

Pour plus de détails sur ce qu'il est possible de faire : iproute2 Cheat Sheet

Des Questions

SEC-LEC : Durcissement sécurité Linux
Identification et authentification

Identification et authentification - Définitions

Les différents concepts présentés dans cette formation sont ceux présentés par le **CISSP** (*Certified Information Systems Security Professional*).

Nous reprendrons aussi un certain nombre de recommandations issues de la norme **ISO 27001**, et celles proposées par l'**ANSSI**.

Identification et authentification - Définitions

CISSP : Certified Information Systems Security Professional

SMSI : ISO 2700X : Système de Management de la Sécurité de l'Information.

- **CIA** : Confidentiality, Intégrity and Avaibility : CIA est un concept
- **(I)AAA** : Identity Authentification, Autorization et Accounting (suivi des logs) : AAA est un ensemble de concepts
- **IAM** : Identification & Autorisation Management: IAM est un outil

Les points précédents seront vus plus en détail dans les slides suivants.

SEC-LEC : Durcissement sécurité Linux

Identification et authentification - Définitions - CIA

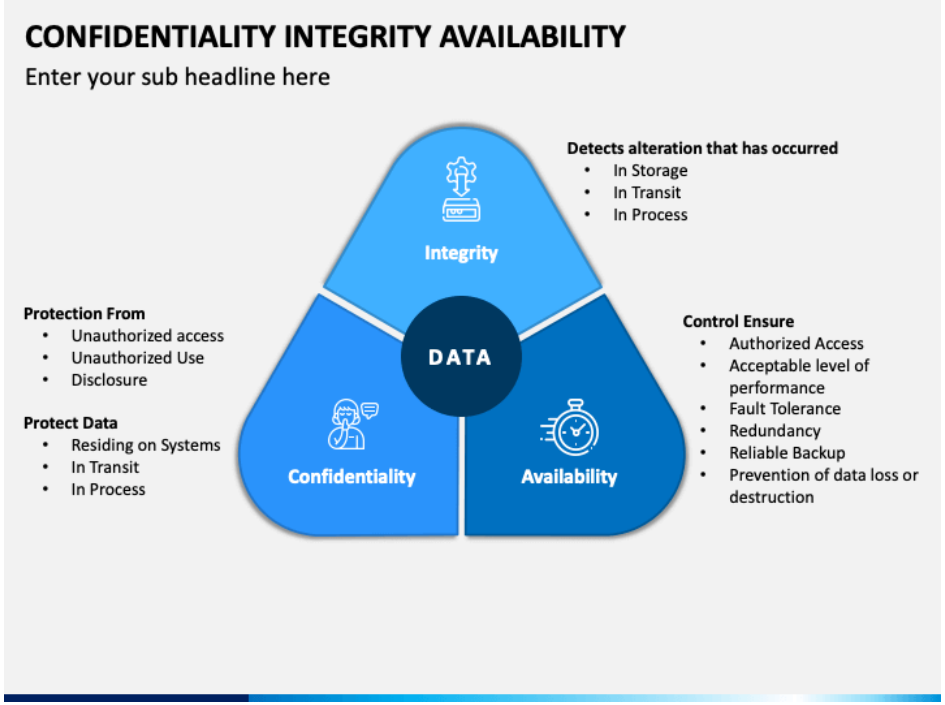
CIA

Confidentiality, Integrity et Availability (Disponibilité) sont les piliers de la sécurité des systèmes d'information.

Ils doivent être documentés dans le PSSI et leur valorisation est définie dans la cartographie des données de l'entreprise.

Confidentiality, Integrity et Availability vont toujours ensemble.

Les concepts IAAA doivent toujours répondre à une valorisation du CIA de chaque donnée.



SEC-LEC : Durcissement sécurité Linux

Identification et authentification - Définitions - Confidentialité

La confidentialité, c'est faire en sorte que **ce qui est secret reste secret**.

Plus précisément, la confidentialité est le fait d'éviter une lecture non autorisée de données. Je dis « données » au sens large, ceci peut-être une fiche de paie comme un plan de bâtiment, un mot de passe ou le nom d'un de vos clients.

On implémente la confidentialité par :

- Le **chiffrement**, vous connaissez, **c'est ce que le commun appelle le « cryptage ».** Cryptage est un anglicisme. « Décrypter » c'est déchiffrer sans avoir la clé.
- Le **masking,** c'est le fait de **masquer des informations confidentielles**,
- La **stéganographie,** c'est le fait de **cacher des informations dans une autre**.

On peut combiner ces éléments ensemble.

On peut appliquer la confidentialité dans les 3 états de la donnée :

- **At Rest** : les données stockées dans un espace de stockage
- **In Transit** : Les données qui circulent dans ou entre des ordinateurs
- **In Process** : Les données sont utilisées par le CPU. Pour produire plus d'informations, les afficher ou les imprimer

Chacun de ces états ont leurs propres façons de cacher le contenu de leur données aux regards non autorisés.

Identification et authentification - Définitions - Intégrité

On a vu que la **confidentialité** traite de la lecture des données, **l'intégrité traite de l'écriture ou modification des données**.

Il y a deux types d'intégrité :

- **Data Integrity : protège les données des modifications non autorisées**. On a alors des données justes auxquelles on peut faire confiance
- **System Integrity : protège un système** tel que Linux **de modifications non autorisées**. On a alors un système stable qui fonctionne comme attendu.

Identification et authentification - Définitions - Disponibilité

À quoi bon avoir des données confidentielles et intègres si on ne peut pas y accéder ? C'est là que la **disponibilité** (availability), trop souvent négligée, entre en jeu.

La disponibilité est l'ensemble des mécanismes rendant des systèmes ou des données accessibles.

- **Redondance** : Le matériel et le logiciel sont munis de mécanisme de redondance
- **Code spécifique** : Le code est spécialement prévu dès le départ pour maintenir sa performance même en cas de problème
- **PCA/PRA** : Un Plan de Continuation d'Activité ou de Reprise d'Activité est conçu afin de maintenir le service associé

Le **SLA** (Service Level Agreement) est un contrat entre un prestataire de service (interne ou externe) et vous-même, garantissant un taux de disponibilité cible d'un système sur une certaine période.

SEC-LEC : Durcissement sécurité Linux

Identification et authentification - Définitions - Disponibilité

Par exemple, un système avec une disponibilité de 99% est en droit de ne pas être disponible un peu plus de 14 minutes par jour sans conséquence financière pour le prestataire.

14 minutes par jour, c'est beaucoup mais rappelez-vous la prochaine fois que vous direz « ça ne marche jamais », on pourrait très bien vous répondre que ça marche 99% du temps…

Taux	Temps d'arrêt par an	Temps d'arrêt par mois
90 %	876h / 36,5j	72h
95 %	438h / 18j	36h
99 %	87:36:00 / 3,5j	7,2h
99,9 %	8:45:36	43,2m
99,99 %	00:52:33,6	4,32m
99,999 %	00:05:15,36	25,9s
99,9999 %	00:00:31,68	2,5s

SEC-LEC : Durcissement sécurité Linux

Identification et authentification - Définitions - (I)AAA

(Identity) Authentification, Autorization et Accounting : Cet ensemble de concepts est souvent, voire toujours, désigné par l'acronyme **AAA** par les différents acteurs du marché de la sécurité. Le I de Identity est alors implicite.

➡ **L'identité**, c'est **qui on prétend être**.

Conceptuellement, c'est le point d'entrée dans la liste des comptes d'utilisateurs, de machines et/ou de services permettant d'en tirer toutes les autres informations.

L'identité est la première étape dans le processus pour accéder à des données.

Identification et authentification - Définitions - (I)AAA

- **L'authentification**, en revanche, est un **mécanisme qui va prouver que la personne qui a clamé son identité est bien elle.**

C'est le moment où un **challenge** est envoyé à l'entité clamant son identité pour valider celle-ci.

Dans la vie courante, ce peut être un document légal d'identité, un mot de passe, ou même juste votre apparence.

On vous reconnait.

C'est aussi valide, même si on ne s'en rend pas compte pour les machines et logiciels.

Autorisation

Ici, ça devient intéressant.

S'être identifié, puis authentifié, induit la mise à disposition d'une liste de droits d'usage autorisés, c'est-à-dire une liste d'actions possibles dans le système dans lequel vous êtes autorisé.

L'autorisation est la production de cette liste de droits. Le menu de ce que vous pouvez faire.

Sortir de cette liste implique que vous ne serez pas autorisé à effectuer l'action souhaitée.

Identification et authentification - Définitions - (I)AAA

Accounting

Ces actions ont laissé des traces dans le système d'accounting de l'entreprise.

Des entrées dans les journaux de logs ont étaient produites provenant de tentatives d'actions infructueuses. Ou même de certaines des actions réussies.

Les **fichiers de logs** sont une mine d'or très peu exploitée par les entreprises. Il faut dire qu'analyser manuellement des millions de lignes n'est pas très digeste.

Ceci pour différentes raisons mais la plus significative est l'investigation forensique.

Comment éviter qu'un incident se reproduise si on n'est pas capable de savoir comment il s'est exactement produit ?

De plus, l'accounting permet de détecter des fraudes en corrélant différents journaux d'événements entre eux.

Identification et authentification - Définitions - (I)AAA

Accounting

Les journaux d'événements permettent également de vérifier que les contrôles de sécurité mis en place fonctionnent comme prévu.

C'est grâce à l'Accounting, que l'on vérifie le System Integrity.

Il faut automatiser la production de sens à l'aide d'outils comme un SIEM, ou d'outils de validation automatique de configuration des serveurs pour sortir du sens de ces logs.

Si augmenter la précision des Logs permet d'augmenter la définition du SIEM, on constate le plus souvent qu'un réglage trop verbeux peut aussi être très contre-productif.

Le rapport signal/bruit devenant trop faible.

SEC-LEC : Durcissement sécurité Linux

Identification et authentification - Définitions - SOC

La famille de logiciels permettant de faciliter la vie des professionnels de la sécurité s'appelle des SIEM (Security Information and Event Management). Le SIEM est donc un outil.

Le **SIEM** est un élément de ce que l'on appelle le SOC (Security Operation Center)

Le **SOC** est le service qui exploite le SIEM à l'aide, entre autres, d'un ensemble de procédures, mais aussi de tableau de bord, d'une cellule de crise et d'une équipe opérationnelle (Réponse à incident, Veille technologique, PenTest,…)

En France, les SOC les plus connus et actifs sont :
Pour le public, celui de ANSSI à Paris, celui du ministère de la défense à Rennes.
Pour le privé, celui d'Orange CyberSécurité, Celui d'Airbus CyberSécurité, ….

De plus en plus d'entreprises se dotent de leurs propres SOC.

SEC-LEC : Durcissement sécurité Linux

Identification et authentification - Définitions - IAM

IAM, ou Identity and Access Management (Gestion d'identité et d'accès), est un ensemble de pratiques et de technologies utilisées pour gérer l'authentification, l'autorisation et la gestion des identités dans un système informatique.

L'objectif de l'IAM est de contrôler l'accès aux ressources informatiques en garantissant que seules les personnes autorisées ont accès à ces ressources.
L'IAM implique la création et la gestion des identités numériques pour les utilisateurs, les groupes et les systèmes informatiques, ainsi que la gestion des autorisations d'accès pour ces identités.

Les systèmes IAM sont couramment utilisés dans les grandes entreprises et les organisations gouvernementales pour gérer l'accès aux ressources informatiques.

SEC-LEC : Durcissement sécurité Linux

Identification et authentification - Définitions - IAM

Les technologies couramment utilisées dans les systèmes IAM comprennent :

- **La gestion des identités** : Comprend la création, la modification et la suppression des identités numériques, ainsi que la gestion des informations d'identification telles que les noms d'utilisateur et les mots de passe.
- **L'authentification** : Permet de vérifier l'identité de l'utilisateur avant de lui accorder l'accès à des ressources.
- **L'autorisation** : Détermine quelles ressources l'utilisateur est autorisé à accéder et à utiliser.
- **L'audit** : Permet de suivre les activités des utilisateurs pour des raisons de conformité et de sécurité.

Ils peuvent être mis en œuvre à l'aide de logiciels propriétaires ou de solutions open source telles que OpenIAM, Keycloak, FreeIPA, ou encore les services IAM proposés par les grands fournisseurs de cloud computing tels que Amazon Web Services, Microsoft Azure ou Google Cloud Platform.

SEC-LEC : Durcissement sécurité Linux

Identification et authentification - Gestion des comptes utilisateurs - Les taches

La gestion des comptes utilisateurs sur un système Linux est une tâche importante pour les administrateurs système. Elle permet de définir les utilisateurs qui ont accès au système, les droits d'accès qui leur sont accordés et les ressources auxquelles ils ont accès.

Voici les principales tâches de gestion des comptes utilisateurs Linux :

- **Création de comptes** : la création d'un compte utilisateur se fait à l'aide de la commande useradd, qui ajoute un nouvel utilisateur à la base de données des utilisateurs. Il est également possible de créer un compte utilisateur avec une interface graphique si elle est disponible.
- **Modification des comptes** : les comptes d'utilisateurs peuvent être modifiés avec la commande usermod. Cette commande permet de modifier divers attributs, tels que le nom complet, le groupe principal, le répertoire personnel, le shell par défaut, etc.
- **Suppression des comptes** : les comptes d'utilisateurs peuvent être supprimés avec la commande userdel. Il est également possible de supprimer le répertoire personnel d'un utilisateur en même temps en utilisant l'option -r.
- **Gestion des mots de passe** : les utilisateurs peuvent définir et modifier leur propre mot de passe avec la commande passwd. Les administrateurs système peuvent également modifier les mots de passe des autres utilisateurs en utilisant la même commande avec des privilèges root.
- **Gestion des groupes** : les utilisateurs sont généralement membres de différents groupes, qui leur permettent d'accéder à des ressources partagées. Les groupes peuvent être créés, modifiés et supprimés à l'aide des commandes groupadd, groupmod et groupdel.
- **Gestion des permissions** : les autorisations d'accès aux fichiers et aux répertoires peuvent être configurées à l'aide des commandes chmod et chown. Ces commandes permettent de définir les autorisations pour les propriétaires, les groupes et les autres utilisateurs.

SEC-LEC : Durcissement sécurité Linux

Identification et authentification - Gestion des comptes utilisateurs - Les fichiers

La gestion des comptes utilisateurs implique la création, la modification et la suppression de plusieurs fichiers qui sont tous nécessaires pour gérer les utilisateurs et leurs droits d'accès.

Voici une brève description des fichiers les plus importants liés à la gestion des comptes utilisateurs sur un système Linux :

- **/etc/passwd** : Contient les informations de base sur les comptes d'utilisateurs du système, tels que leur nom d'utilisateur, leur UID (User ID), leur GID (Group ID), leur nom complet et leur répertoire personnel. Ce fichier peut être consulté par tous les utilisateurs du système.
- **/etc/shadow** : Contient les informations de sécurité des comptes d'utilisateurs, telles que les mots de passe chiffrés et la date de dernière modification du mot de passe. Ce fichier est accessible uniquement par l'utilisateur root.
- **/etc/group** : Contient la liste des groupes d'utilisateurs et les utilisateurs qui en font partie. Chaque groupe a un nom et un GID, et les utilisateurs peuvent être membres de plusieurs groupes. Ce fichier peut être consulté par tous les utilisateurs du système.
- **/etc/skel/** : Contient les fichiers et les dossiers qui seront copiés dans le répertoire personnel de chaque nouvel utilisateur créé sur le système.
- **/etc/login.defs** : Contient les paramètres de configuration pour le système de connexion. Il définit, entre autres, les politiques de mot de passe, les messages d'erreur, les limites de connexion et les directives de verrouillage de compte.
- **/home/** : Contient le répertoire personnel de chaque utilisateur créé sur le système.

En résumé, la gestion des comptes utilisateurs sur un système Linux implique la création, la modification et la suppression de plusieurs fichiers, y compris /etc/passwd, /etc/shadow, /etc/group, /etc/skel, /etc/login.defs et /home. Ces fichiers contiennent des informations de base sur les comptes d'utilisateurs, les informations de sécurité, la liste des groupes d'utilisateurs et les fichiers de configuration nécessaires pour le système de connexion.

Identification et authentification - Gestion des comptes utilisateurs - Les fichiers

/etc/passwd

```
gerard:x:1000:1000:Gerard,,,:/home/gerard:/bin/bash
```

1. nom de l'utilisateur
2. mot de passe (x signifie qu'il se trouve dans /etc/shadow)
3. UID : O=root, 0<UID<999 compte système,>=1000 utilisateur normal
4. GID : Groupe primaire (voir /etc/group)
5. GECOS : Information complémentaire (finger)
6. Home directory
7. Command/Shell (souvent un des shell notés dans /etc/shells, mais peut être n'importe quoi d'autre comme /sbin/nologin)

/etc/passwd

Lister les utilisateurs connus du système : **getent passwd**

Créer un utilisateur, son groupe et son mot de passe : **useradd test**

Supprimer un utilisateur : **userdel test**

Ajouter -r à la commande va supprimer le home directory en même temps.

On donne des droits root à un utilisateur en l'ajoutant dans le group sudo : **usermod -aG sudo test**

Le groupe s'appelle wheel dans la famille de distributions redhat.

/etc/group

egersec:x:1003:gerard,emmanuel,cathia

1. Nom du groupe
2. Mot de passe
3. GID : Identifiant de groupe
4. Groupe list : liste séparé par une virgule des membres d'un groupe.

La commande id permet de visualiser cette information pour un utilisateur :

:/etc$ id
uid=1000(gerard) gid=1000(gerard)
groups=1000(gerard),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),114(sambashare),1003(egersec)

/etc/group

Lister les groupes du système : **getent group**

De la même façon que pour les utilisateurs, il existe des **groupadd**, **groupdel** et **groupmod**.

/etc/shadow

```
nobody:*:18348:0:99999:7:::
```

Les champs sont séparés par des :

Les dates sont en nombre de jours depuis le 1 janvier 1970.

1. Nom du compte
2. Mot de passe de la forme idsalt$hashed ou contenant ! ou *, pour respectivement un compte ou un service locké.
3. Date du dernier changement de mot de passe (0 : changement obligatoire)
4. Nombre minimum de jours entre les différents changement de mot de passe (0 : pas de minimum)
5. Nombre maximum de jours entre les différents changement de mot de passe
6. Nombre de jours d'attente après la fin de validité du mot de passe
7. Nombre de jours d'attente après la fin de validité du mot de passe avec blocage de connexion.
8. Date d'expiration du compte

/etc/shadow

La partie id du point 2. du slide précédent peut avoir les valeurs suivantes :

- 1 : MD5
- 2 : Blowfish
- 5 : SHA-256
- 6 : SHA-512
- y : Yescrypt

/etc/shadow

Il est possible de tester la difficulté de cracker un mot de passe en utilisant **john the ripper** et la base mots de passe standard **rockyou.txt.**

apt install john

wget https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt

Puis on remplace les x par les hash correspondant :

sudo unshadow /etc/passwd /etc/shadow > unshadowed

john --wordlist=rockyou.txt unshadowed

Gestion des mots de passe

Les mots de passe dont changés à l'aide de la commande **passwd.**

$ passwd
 # passwd formation

La durée de vie d'un mot de passe est suivie avec la commande **chage.**

$ chage -l

La commande **pwck** va permettre de valider l'intégrité de toute la base de données des comptes et mots de passe.

$ sudo pwck
user 'lp': directory '/var/spool/lpd' does not exist
user 'news': directory '/var/spool/news' does not exist
user 'uucp': directory '/var/spool/uucp' does not exist
user 'list': directory '/var/list' does not exist
user 'irc': directory '/run/ircd' does not exist
user 'gnats': directory '/var/lib/gnats' does not exist
pwck: no changes

/etc/login.defs

Le fichier de paramètrage /etc/logins.defs contient les paramètres permettant de gérer les mots de passes.

```
#
# Password aging controls:
#
#       PASS_MAX_DAYS   Maximum number of days a password may be used.
#       PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#       PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_WARN_AGE   7
```

SEC-LEC : Durcissement sécurité Linux

Identification et authentification - Gestion des comptes utilisateurs

Le compte root est le compte super-utilisateur sur les systèmes Unix et Linux. Il a tous les privilèges et peut effectuer toutes les tâches sur le système. En raison de ces privilèges élevés, il est recommandé de ne pas utiliser le compte root pour des tâches courantes et d'utiliser plutôt la commande sudo.

Sudo est une commande Unix qui permet à un utilisateur de bénéficier temporairement des privilèges du compte root pour exécuter des tâches spécifiques. L'utilisation de sudo permet d'exécuter des commandes en tant qu'utilisateur normal avec des privilèges limités, mais d'accéder temporairement aux privilèges de super-utilisateur pour effectuer des tâches spécifiques qui nécessitent des privilèges élevés.

Voici quelques bonnes pratiques pour gérer le compte root et utiliser la commande sudo :

- **Ne pas utiliser le compte root pour les tâches courantes** : Il est recommandé de n'utiliser le compte root que pour les tâches qui nécessitent des privilèges élevés, comme l'installation de logiciels ou la configuration du système.
- **Créer un utilisateur administrateur** : Il est recommandé de créer un utilisateur avec des privilèges d'administration pour effectuer les tâches courantes qui ne nécessitent pas les privilèges de super-utilisateur.
- **Utiliser la commande sudo** : Utilisez la commande sudo pour effectuer des tâches qui nécessitent des privilèges élevés. Pour utiliser sudo, tapez la commande sudo suivi de la commande à exécuter en tant que super-utilisateur.
- **Utiliser la configuration sudoers** : La configuration sudoers permet de définir les utilisateurs et les groupes autorisés à utiliser la commande sudo et les commandes spécifiques qu'ils sont autorisés à exécuter en tant que super-utilisateur. Il est recommandé de configurer sudoers de manière appropriée pour éviter les abus et les erreurs.
- **Restreindre l'accès à la commande sudo** : Il est recommandé de restreindre l'accès à la commande sudo aux utilisateurs et groupes de confiance pour éviter les abus et les erreurs.
- **Interdire le mot de passe pour le compte root** : Il est recommandé d'interdire le mot de passe pour le compte root afin d'empêcher toute connexion directe en tant que super-utilisateur. Cela permet de limiter les risques de sécurité en limitant les possibilités d'accès non autorisé. De cette façon, les utilisateurs doivent se connecter en tant qu'utilisateur standard, puis utiliser la commande sudo pour accéder temporairement aux privilèges de super-utilisateur.
- **Interdiction de se connecter à distance directement en tant que root** : Il est fortement recommandé d'interdire la connexion à distance en tant que compte root sur un système. Cette mesure de sécurité permet de limiter les risques d'attaques par force brute ou par attaques de dictionnaires, qui peuvent être utilisées pour casser un mot de passe root. Cela permet de faciliter la traçabilité des actions effectuées par les utilisateurs, en enregistrant les informations de connexion et d'utilisation des commandes.

En suivant ces bonnes pratiques, vous pouvez améliorer la sécurité de votre système en réduisant les risques d'abus de privilèges du compte root et en utilisant la commande sudo de manière sécurisée.

SEC-LEC : Durcissement sécurité Linux

Identification et authentification - Pluggable Authentication Modules (PAM)

Pluggable Authentication Modules (PAM) est un système d'authentification modulaire pour les systèmes d'exploitation Linux et Unix. Il permet à différents types d'authentification d'être utilisés par des applications sur le système, tels que l'authentification par mot de passe, l'authentification par carte à puce, ou encore l'authentification biométrique.

PAM fournit un cadre pour l'authentification des utilisateurs, la gestion des mots de passe, la gestion des sessions, et la gestion des autorisations pour les applications qui le supportent. Les modules PAM peuvent être configurés pour exécuter des actions spécifiques en fonction de différentes conditions, telles que le moment de la journée, l'adresse IP de l'utilisateur, ou encore l'application utilisée.

Les modules PAM sont généralement configurés dans les fichiers de configuration situés dans le répertoire /etc/pam.d/ sur le système. Chaque fichier de configuration correspond à une application ou un service spécifique et contient une liste de modules PAM qui doivent être exécutés pour cette application ou ce service. Chaque module PAM peut définir des règles pour l'authentification de l'utilisateur, la gestion des sessions ou des autorisations.

PAM permet de mettre en place des politiques de sécurité avancées pour les systèmes d'exploitation en permettant aux administrateurs de configurer des règles d'authentification et d'autorisation spécifiques pour chaque application ou service sur le système. Les administrateurs peuvent ainsi imposer des règles de sécurité spécifiques pour chaque application, en fonction de ses exigences de sécurité.

On peut s'authentifier en liaison avec les fichiers dans /etc/, LDAP, un lecteur d'empreinte digitale.

Identification et authentification - Pluggable Authentication Modules (PAM)

Les modules PAM (Pluggable Authentication Modules) sont des composants logiciels qui fournissent les fonctionnalités d'authentification, d'autorisation et de gestion de session pour les applications qui utilisent le système d'authentification PAM.

Les modules PAM peuvent être configurés pour répondre à des politiques de sécurité spécifiques, permettant aux administrateurs système de mettre en place des règles d'authentification et d'autorisation spécifiques pour chaque application ou service sur le système.

Les modules PAM sont regroupés en trois types principaux:

- **Modules d'authentification** : Ces modules sont utilisés pour authentifier les utilisateurs lors de leur connexion. Ils fournissent des fonctionnalités telles que la vérification des noms d'utilisateur et des mots de passe, l'authentification par carte à puce, l'authentification biométrique, etc.
- **Modules d'autorisation** : Ces modules sont utilisés pour déterminer si un utilisateur est autorisé à effectuer une action spécifique, telle que l'accès à un fichier ou à un répertoire. Ils fournissent des fonctionnalités telles que la vérification de l'appartenance à un groupe, la vérification des ACL (Access Control List), la vérification de l'adresse IP, etc.
- **Modules de gestion de session** : Ces modules sont utilisés pour gérer les sessions utilisateur, tels que la création de répertoires de travail, la définition de variables d'environnement, la gestion des connexions réseau, etc.

Identification et authentification - Pluggable Authentication Modules (PAM)

Voici quelques exemples de modules PAM pour les trois types principaux :

Modules d'authentification:

- **pam_unix** : C'est le module PAM d'authentification de base qui vérifie les noms d'utilisateur et les mots de passe stockés localement sur le système. Il utilise le fichier /etc/passwd pour les noms d'utilisateur et le fichier /etc/shadow pour les mots de passe.
- **pam_ssh** : Ce module PAM permet aux utilisateurs de s'authentifier à l'aide de leurs clés SSH. Il peut être utilisé pour permettre l'authentification sans mot de passe à travers SSH.
- **pam_pkcs11** : Ce module PAM permet l'authentification par carte à puce. Il peut être utilisé pour permettre aux utilisateurs de s'authentifier à l'aide de leurs cartes à puce.

Modules d'autorisation:

- **pam_access** : Ce module PAM permet de définir des règles d'accès pour les utilisateurs et les groupes. Il peut être utilisé pour restreindre l'accès à certains services ou fichiers en fonction des groupes d'utilisateurs ou des adresses IP.
- **pam_limits** : Ce module PAM permet de définir des limites d'utilisation de ressources système pour les utilisateurs. Il peut être utilisé pour restreindre la quantité de mémoire ou de CPU qu'un utilisateur peut utiliser.
- **pam_time** : Ce module PAM permet de définir des règles basées sur le temps d'accès pour les utilisateurs. Il peut être utilisé pour restreindre l'accès à certains services ou fichiers en fonction de l'heure de la journée.

Modules de gestion de session:

- **pam_mkhomedir** : Ce module PAM crée automatiquement le répertoire de travail de l'utilisateur lors de sa première connexion. Il peut être utilisé pour simplifier la création de comptes d'utilisateurs.
- **pam_env** : Ce module PAM permet de définir des variables d'environnement pour la session de l'utilisateur. Il peut être utilisé pour ajouter des variables spécifiques pour chaque utilisateur, ou pour définir des variables d'environnement globales.
- **pam_systemd** : Ce module PAM permet de contrôler les services système avec systemd. Il peut être utilisé pour redémarrer ou arrêter des services système lors de l'ouverture ou de la fermeture de session utilisateur.

SEC-LEC : Durcissement sécurité Linux

Identification et authentification - Pluggable Authentication Modules (PAM)

Les fichiers de configuration PAM sont généralement stockés dans le répertoire /etc/pam.d et contiennent des lignes qui définissent les modules PAM et leurs options pour chaque service. Chaque ligne est composée de plusieurs champs, séparés par des espaces.

Voici la signification et les valeurs possibles de chaque champ :

Champ 1 : Type de service

Ce champ spécifie le type de service qui utilise ce fichier de configuration. Il peut s'agir d'un nom de service prédéfini tel que login, ssh ou sudo, ou d'un nom de service personnalisé.

Champ 2 : Type de contrôle

Ce champ spécifie le type de contrôle d'accès utilisé pour le service. Les valeurs possibles sont :

- **auth**: Contrôle l'authentification de l'utilisateur
- **account**: Contrôle les politiques de compte pour l'utilisateur
- **password**: Contrôle la mise à jour du mot de passe de l'utilisateur
- **session**: Contrôle la gestion de session de l'utilisateur

Champ 3 : Nom du module

Ce champ spécifie le nom du module PAM qui sera utilisé pour le service.

Champ 4 : Options du module

Ce champ spécifie les options de configuration pour le module PAM. Les options peuvent varier en fonction du module spécifié.

Les valeurs possibles pour les options de configuration dépendent du module utilisé. Voici quelques exemples d'options pour certains modules couramment utilisés :

- **pam_unix** : nullok, use_first_pass, try_first_pass, debug
- **pam_access** : accessfile, debug
- **pam_limits** : limit, debug
- **pam_time** : access.conf, debug

Le champ d'option est facultatif et n'est pas toujours présent. S'il est présent, il peut être utilisé pour configurer le comportement du module PAM

SEC-LEC : Durcissement sécurité Linux

Identification et authentification - Les niveaux de sécurité PAM

Il n'y a pas de niveaux de sécurité prédéfinis dans PAM, car le niveau de sécurité dépend des modules PAM utilisés et de la manière dont ils sont configurés pour un service donné. Cependant, il est possible de configurer PAM pour fournir des niveaux de sécurité personnalisés en utilisant une combinaison de modules et d'options.

Voici quelques exemples de niveaux de sécurité que vous pouvez implémenter avec PAM :

- **Authentification forte** : Pour une authentification forte, vous pouvez configurer PAM pour utiliser des méthodes d'authentification plus robustes que le simple nom d'utilisateur et mot de passe, telles que les clés SSH, les jetons à usage unique (OTP) ou les certificats numériques.
- **Contrôle d'accès renforcé :** Vous pouvez configurer PAM pour utiliser des modules tels que pam_access pour appliquer des règles de contrôle d'accès plus strictes. Par exemple, vous pouvez définir des règles pour interdire l'accès à certains utilisateurs ou groupes à des heures spécifiques ou à partir de certaines adresses IP
- **Détection et prévention des attaques :** Vous pouvez utiliser des modules PAM tels que pam_tally2 pour suivre les tentatives de connexion infructueuses et verrouiller les comptes d'utilisateur en cas de nombre excessif de tentatives échouées. Vous pouvez également utiliser des modules tels que pam_cracklib pour définir des politiques de mot de passe plus strictes et empêcher l'utilisation de mots de passe faibles
- **Audit et surveillance** : En utilisant des modules PAM tels que pam_unix avec l'option audit, vous pouvez enregistrer des informations d'audit pour chaque connexion réussie ou échouée. Vous pouvez également utiliser des outils de surveillance de l'intégrité tels que AIDE ou Tripwire pour surveiller les fichiers système et les journaux PAM pour détecter les activités suspectes.

Ces exemples ne sont pas exhaustifs et la façon dont vous configurez PAM dépendra des besoins de sécurité de votre système. Cependant, en utilisant une combinaison de modules et d'options, vous pouvez personnaliser le niveau de sécurité PAM pour répondre aux exigences de sécurité de votre système.

SEC-LEC : Durcissement sécurité Linux

Identification et authentification - Les OTP (Sécurité Hardware et Software)

OTP signifie "One-Time Password" ou "Mot de passe à usage unique".

Il s'agit d'une méthode d'authentification qui génère des codes de sécurité uniques à usage unique pour chaque connexion ou transaction, afin de renforcer la sécurité du processus d'authentification. Il existe deux types d'OTP : les solutions matérielles et les solutions logicielles.

- Les solutions matérielles OTP utilisent des tokens physiques, tels que des clés USB, des cartes à puce ou des jetons électroniques, qui génèrent des codes à usage unique pour l'authentification. Les utilisateurs doivent généralement insérer le token dans un port USB ou le tenir près d'un lecteur NFC pour que le code OTP soit généré. Les solutions matérielles OTP sont généralement plus coûteuses que les solutions logicielles, mais elles sont également plus sûres car les tokens sont difficiles à pirater ou à compromettre.
- Les solutions logicielles OTP sont des applications installées sur un ordinateur, un téléphone portable ou une tablette, qui génèrent des codes à usage unique pour l'authentification. Les codes peuvent être générés à partir d'une application tierce, d'un SMS ou d'un courriel. Les solutions logicielles OTP sont généralement moins coûteuses que les solutions matérielles, mais elles sont également moins sécurisées car elles sont vulnérables aux attaques de logiciels malveillants, aux attaques par hameçonnage et à d'autres formes de piratage.

En général, les solutions OTP offrent une sécurité supplémentaire pour les systèmes nécessitant une authentification forte, tels que les services bancaires en ligne, les services de paiement et les systèmes de gestion d'entreprise. Cependant, les solutions OTP ne sont pas parfaites et peuvent être contournées en cas de vol ou de perte de tokens physiques ou de compromission de l'application logicielle. Par conséquent, il est important de combiner les solutions OTP avec d'autres méthodes de sécurité, telles que des mots de passe forts, des politiques de sécurité strictes et une surveillance continue des activités suspectes.

SEC-LEC : Durcissement sécurité Linux

Identification et authentification - Les OTP (Sécurité Hardware et Software)

HOTP et TOTP sont deux types d'algorithmes utilisés pour générer des codes à usage unique (OTP) dans le cadre de systèmes d'authentification forte basés sur des OTP :

- **HOTP signifie "HMAC-based One-Time Password"** et est basé sur une fonction de hachage cryptographique. Il fonctionne en utilisant une clé secrète partagée entre l'utilisateur et le serveur d'authentification. Lors de chaque demande d'authentification, le serveur envoie un numéro de séquence à l'utilisateur qui l'utilise avec la clé secrète pour générer un code HOTP unique. Le serveur peut alors vérifier le code reçu de l'utilisateur en utilisant la même clé secrète et le même numéro de séquence.
- **TOTP signifie "Time-based One-Time Password"** et est également basé sur une fonction de hachage cryptographique. Il fonctionne de manière similaire à HOTP, sauf que le code OTP est généré en utilisant l'heure actuelle plutôt qu'un numéro de séquence. L'utilisateur et le serveur partagent une clé secrète et un paramètre de temps, et l'utilisateur utilise cette information pour générer un code TOTP unique à chaque demande d'authentification.

Les deux méthodes, HOTP et TOTP, offrent un haut niveau de sécurité et sont largement utilisées dans les systèmes d'authentification forte, notamment dans les systèmes de gestion de mots de passe, les applications de sécurité bancaire et les solutions d'authentification multifactorielle.

Les codes OTP générés par HOTP et TOTP sont valables pour une seule utilisation et ont une durée de validité limitée, ce qui rend leur utilisation plus sûre que les mots de passe statiques.

Cependant, il est important de garder à l'esprit que ces solutions ne sont pas parfaites et peuvent être compromises si les clés secrètes sont volées ou si les paramètres de temps sont décalés.

SEC-LEC : Durcissement sécurité Linux

Identification et authentification - Les OTP (Sécurité Hardware et Software)

Pour configurer SSH avec TOTP et utiliser une application de téléphone pour générer des codes TOTP, vous devez suivre les étapes suivantes :

- Installez la librairie Google Authenticator sur votre serveur Linux en utilisant la commande suivante :
  sudo apt install libpam-google-authenticator
- Générez une clé secrète en utilisant la commande suivante :
  google-authenticator

Cette commande vous guidera à travers un processus interactif pour générer une clé secrète et configurer l'authentification TOTP pour votre compte utilisateur.

- Ajoutez la configuration PAM nécessaire pour utiliser l'authentification TOTP avec SSH en modifiant le fichier /etc/pam.d/sshd. Ajoutez les lignes suivantes au début du fichier :
  # Utiliser Google Authenticator PAM

  auth required pam_google_authenticator.so
- Redémarrez le service SSH en utilisant la commande suivante :
  sudo service sshd restart
- Installez une application de téléphone compatible TOTP sur votre téléphone. Vous pouvez utiliser des applications comme Google Authenticator, Microsoft Authenticator ou FreeOTP.
- Scannez le code QR ou entrez la clé secrète générée précédemment dans l'application de téléphone. L'application de téléphone générera des codes TOTP à usage unique.

Lorsque vous vous connectez à votre serveur via SSH, entrez votre nom d'utilisateur et votre mot de passe, puis saisissez le code TOTP généré par l'application de téléphone.

Cela devrait vous permettre de configurer SSH avec l'authentification TOTP et d'utiliser une application de téléphone pour générer des codes TOTP pour l'authentification. Il est important de noter que chaque application de téléphone peut avoir une interface légèrement différente pour ajouter un compte TOTP, mais les étapes de base devraient être similaires pour la plupart des applications de ce type.

Des Questions

SEC-LEC : Durcissement sécurité Linux
Déploiement du système Linux

SEC-LEC : Durcissement sécurité Linux

Protection des fichiers - Droits standards des systèmes de fichiers Unix

Les systèmes de fichiers Unix sont conçus pour être multi-utilisateurs et multi-tâches, de sorte que les fichiers sont généralement associés à des permissions qui définissent les droits d'accès pour chaque utilisateur ou groupe. Les droits d'accès aux fichiers sont divisés en trois catégories : propriétaire, groupe et autres.

Ces droits d'accès sont définis pour trois types d'utilisateurs :

- **Propriétaire** (User: U) : l'utilisateur qui a créé le fichier ou le répertoire
- **Groupe** (Group : G) : un ensemble d'utilisateurs qui partagent les mêmes droits d'accès
- **Autres** (Other : O) : tous les autres utilisateurs

Les droits d'accès pour chaque utilisateur sont spécifiés en utilisant une notation en trois caractères. Le premier caractère indique les droits d'accès pour le propriétaire, le deuxième pour le groupe, et le troisième pour les autres. Les droits d'accès sont représentés par les caractères suivants :

- **r** : lecture
- **w** : écriture
- **x** : exécution
- **-** : pas d'accès

Par exemple, la notation "rwxr-xr--" indique que le propriétaire a tous les droits (lecture, écriture, exécution), les membres du groupe ont le droit de lire et d'exécuter, et les autres utilisateurs n'ont que le droit de lire.

En outre, les droits standards peuvent être étendus à l'aide de certaines options, notamment :

- **Setuid** (s) : lorsqu'un fichier est marqué avec ce bit, il est exécuté avec les privilèges du propriétaire du fichier plutôt que de l'utilisateur qui l'a exécuté.
- **Setgid** (s) : lorsqu'un répertoire est marqué avec ce bit, les fichiers créés dans le répertoire héritent du groupe de ce répertoire plutôt que du groupe de l'utilisateur qui les a créés.
- **Sticky** bit (t) : lorsqu'un répertoire est marqué avec ce bit, les utilisateurs ne peuvent pas supprimer les fichiers créés par d'autres utilisateurs, sauf s'ils sont propriétaires ou administrateurs du système.

Ces options sont souvent utilisées pour renforcer la sécurité du système de fichiers Unix.

Protection des fichiers - Droits standards des systèmes de fichiers Unix

```
$ ls -ltr
total 104
drwxrwxr-x 5 gerard gerard  4096 Oct 16  2020 wiki
drwxrwxr-x 4 gerard gerard  4096 Jan  4  2021 upload
-rw-rw-r-- 1 gerard gerard 73198 Dec 23  2021 Egersec-transparent.png
lrwxrwxrwx 1 gerard gerard    10 Feb  2  2022 egersec -> ../egersec
drwxrwxr-x 2 gerard gerard  4096 May 12 14:11 DATA
-rw-r--r-- 1 root   root   14323 May 26 13:01 install-tr-control.sh
drwx------ 2 gerard gerard  4096 Aug 31 09:31 Downloads
```

Droits standards des systèmes de fichiers Unix

On change le propriétaire et le group associé au fichier avec la commande chown

```
 :~/test$ ls -l
total 0
-rw-rw-r--  1 gerard gerard 0 Sep  3 19:31 owner
 :~/test$ sudo chown cathia:cathia owner
 :~/test$ ls -l
total 0
-rw-rw-r--  1 cathia cathia 0 Sep  3 19:31 owner
 :~/test$
```

Protection des fichiers - Droits standards des systèmes de fichiers Unix

Droits standards des systèmes de fichiers Unix

On change les droits sur un fichier à l'aide de la commande chmod

```
 :~/test$ ls -l
total 0
-rw-rw-r--  1 cathia cathia 0 Sep  3 19:31 owner
 :~/test$ sudo chmod a+x owner
 :~/test$ ls -l
total 0
-rwxrwxr-x  1 cathia cathia 0 Sep  3 19:31 owner
 :~/test$
```

Protection des fichiers - Les listes de contrôle d'accès

Les **listes de contrôle d'accès** getfacl/setfacl (get file access control list/set file access control list) sont des outils pour gérer les permissions des fichiers et des répertoires dans les systèmes de fichiers Unix.

La liste de contrôle d'accès (ACL) est un ensemble d'attributs supplémentaires qui peut être ajouté à un fichier ou un répertoire pour définir des permissions plus précises que celles offertes par les droits d'accès standards des systèmes de fichiers Unix.

- La commande **getfacl** permet de récupérer les ACL d'un fichier ou d'un répertoire et de les afficher sous forme de texte. La sortie affiche les différents utilisateurs et groupes définis dans les ACL, ainsi que les autorisations spécifiques accordées à chacun. Par exemple, la commande getfacl fichier affiche les ACL du fichier nommé "fichier"
- La commande **setfacl** permet de modifier les ACL d'un fichier ou d'un répertoire en utilisant un ensemble de règles pré-définies. Par exemple, la commande setfacl -m u:utilisateur:rwx fichier permet de donner à l'utilisateur "utilisateur" les permissions de lecture, écriture et exécution sur le fichier nommé "fichier"

Les ACL peuvent également être définis pour les groupes, les utilisateurs anonymes et les utilisateurs qui n'appartiennent pas à un groupe donné. Les ACL peuvent être utilisées pour définir des permissions spécifiques pour des utilisateurs individuels, même s'ils ne sont pas membres du groupe propriétaire du fichier.

Les ACL offrent une flexibilité accrue pour la gestion des autorisations de fichiers et de répertoires, et peuvent être utilisées en combinaison avec les droits d'accès standards des systèmes de fichiers Unix pour fournir une sécurité granulaire et fine.

Les exemples de manipulation se trouvent dans le fichier ACL.list.

Protection des fichiers - Les listes de contrôle d'accès

Il est possible de copier le contenu d'un répertoire en en conservant ses ACL :

- Extraire l'information du contenu en ACL du répertoire : *getfacl -R /a_folder > folder.acl*
- Faire un tar normal : *tar -czvf folder.tar.gz /a_folder*
- Le déplacer, l'extraire au bon endroit : *tar -xvf folder.tar.gz*
- Appliquer les ACL contenu dans le fichier extrait : *setfacl --restore=folder.acl*

Ou, sinon, rsync avec les bons paramètres en est aussi capable :

- *rsync -aAX /source/filename /destination/newfilename*

SEC-LEC : Durcissement sécurité Linux

Protection des fichiers - Les attributs étendus

Les attributs étendus, ou xattr, sont des méta-données qui peuvent être ajoutées à des fichiers et des répertoires dans les systèmes de fichiers Unix. Ils permettent de stocker des informations supplémentaires sur un fichier ou un répertoire, telles que des notes, des commentaires, des méta-données, des informations de version, etc.

Les commandes **lsattr** et **chattr** sont utilisées pour afficher et modifier les attributs étendus d'un fichier ou d'un répertoire.

- La commande lsattr affiche les attributs étendus existants d'un fichier ou d'un répertoire. Les attributs sont affichés avec un indicateur "+" pour chaque attribut présent. Par exemple, la commande lsattr fichier affiche les attributs étendus du fichier nommé "fichier".
- La commande chattr permet de modifier les attributs étendus d'un fichier ou d'un répertoire. Les attributs peuvent être ajoutés, supprimés ou modifiés en utilisant une série d'options pré-définies.

SEC-LEC : Durcissement sécurité Linux

Protection des fichiers - Les attributs étendus

Les options les plus courantes sont :

- **a (append only)** : permet d'ajouter des données à la fin d'un fichier sans pouvoir les modifier ou les supprimer.
- **c (compressed)** : permet de compresser un fichier lorsqu'il est stocké sur le disque.
- **d (no dump)** : permet d'indiquer au programme de sauvegarde de ne pas inclure le fichier ou le répertoire dans la sauvegarde.
- **i (immutable)** : empêche toute modification ou suppression du fichier.
- **j (journal)** : permet d'activer la journalisation des données pour le fichier.
- **s (secure deletion)** : permet de supprimer de manière sécurisée le contenu d'un fichier en écrivant des zéros sur l'espace disque occupé.
- **t (no tail-merging)** : empêche la fusion des données des fichiers avec des blocs de données adjacents sur le disque.
- **u (undeletable)** : permet de récupérer un fichier supprimé.

Les **modes possibles de la commande chattr** sont les suivants :

- **+ (ajout)** : ajoute l'attribut spécifié au fichier ou au répertoire.
- **- (suppression)** : supprime l'attribut spécifié du fichier ou du répertoire.
- **= (remplacement)** : remplace tous les attributs existants par les attributs spécifiés.

SEC-LEC : Durcissement sécurité Linux

Protection des fichiers - Les attributs étendus

Les attributs étendus

```
 :~/test$ ls -ltr myattr
-rw-rw-r-- 1 gerard gerard 0 Sep  4 12:26 myattr
 :~/test$ lsattr myattr
--------------e------- ./myattr
 :~/test$ sudo chattr +i myattr
 :~/test$ lsattr myattr
----i---------e------- ./myattr
  :~/test$ rm myattr
rm: cannot remove 'myattr': Operation not permitted
 :~/test$ ls -ltr myattr
-rw-rw-r-- 1 gerard gerard 0 Sep  4 12:26 myattr
 :~/test$ sudo chattr -i myattr
 :~/test$ rm myattr
 :~/test$ ls -ltr myattr
ls: cannot access 'myattr': No such file or directory
```

SEC-LEC : Durcissement sécurité Linux

Protection des fichiers - Vérification de l'intégrité d'un système de fichiers

Dans Linux, la vérification de l'intégrité du système de fichiers peut être effectuée à l'aide de la commande "fsck" (pour "file system check") qui est un outil en ligne de commande pour vérifier et réparer les systèmes de fichiers corrompus ou endommagés.

Il est recommandé de vérifier l'intégrité du système de fichiers lors du démarrage du système. Pour cela, il est possible d'utiliser systemd, le système d'initialisation par défaut de nombreuses distributions Linux.

Voici comment configurer systemd pour vérifier automatiquement l'intégrité du système de fichiers au démarrage :

- Ouvrez un terminal et éditez le fichier /etc/fstab en tant que root :

  sudo vi /etc/fstab

- Trouvez la ligne correspondant à la partition racine ("/") et ajoutez "0 1" à la fin de la ligne. Cela indique à systemd de vérifier le système de fichiers au démarrage. Par exemple :

  /dev/sda1 / ext4 defaults 0 1

- Sauvegardez et fermez le fichier.
- Éditez le fichier /etc/default/grub en tant que root :

  sudo vi /etc/default/grub

- Trouvez la ligne GRUB_CMDLINE_LINUX et ajoutez "fsck.mode=force" à la fin de la ligne. Cela indique à systemd de forcer la vérification du système de fichiers au démarrage. Par exemple :

  GRUB_CMDLINE_LINUX="quiet splash fsck.mode=force"

- Sauvegardez et fermez le fichier.
- Mettez à jour le chargeur de démarrage GRUB en exécutant la commande suivante :

  sudo update-grub

Redémarrez votre système. La vérification du système de fichiers doit maintenant être effectuée automatiquement au démarrage

Protection des fichiers - Vérification de l'intégrité d'un système de fichiers

Il est également possible de configurer systemd pour effectuer des vérifications régulières du système de fichiers en utilisant des timers.

Par exemple, pour vérifier le système de fichiers toutes les semaines, vous pouvez créer un fichier de configuration de timer dans le répertoire /etc/systemd/system/ avec le contenu suivant :

```
[Unit]
Description=Weekly
File System Check

[Timer]
OnCalendar=weekly
AccuracySec=1min
Persistent=true

[Install]
WantedBy=timers.target
```

➡ Sauvegardez le fichier en tant que "fsck.timer" et rechargez la configuration systemd en exécutant la commande suivante :

sudo systemctl daemon-reload

➡ Ensuite, activez et démarrez le timer en utilisant les commandes suivantes :

sudo systemctl enable --now fsck.timer

Cela configure systemd pour effectuer une vérification du système de fichiers chaque semaine.

Protection des fichiers - Le chiffrement des fichiers

Le chiffrement des fichiers est un moyen de sécuriser les données en les transformant à l'aide d'un algorithme mathématique pour rendre leur contenu illisible sans une clé de déchiffrement appropriée.

Il existe plusieurs méthodes de chiffrement de fichiers, mais la plupart utilisent des algorithmes de chiffrement symétriques ou asymétriques.

- **Dans le chiffrement symétrique**, une même clé est utilisée pour chiffrer et déchiffrer les données.
- **Dans le chiffrement asymétrique**, deux clés différentes (une clé publique et une clé privée) sont utilisées pour chiffrer et déchiffrer les données.

Voici les étapes générales pour chiffrer des fichiers :

- **Choisir un algorithme de chiffrement approprié.** Il existe de nombreux algorithmes de chiffrement différents, chacun avec ses propres avantages et inconvénients. Les algorithmes populaires incluent AES, Blowfish et RSA.
- **Générer une clé de chiffrement.** Dans le chiffrement symétrique, vous devez générer une clé de chiffrement qui sera utilisée pour chiffrer et déchiffrer les données. Dans le chiffrement asymétrique, vous devez générer une paire de clés : une clé publique et une clé privée. La clé publique est utilisée pour chiffrer les données, tandis que la clé privée est utilisée pour les déchiffrer.
- **Chiffrer les fichiers.** Utilisez l'algorithme de chiffrement et la clé de chiffrement ou la clé publique pour chiffrer les fichiers.
- **Stocker la clé de chiffrement ou la clé privée en lieu sûr**. Dans le chiffrement symétrique, la clé de chiffrement doit être stockée en lieu sûr, car toute personne qui la possède peut accéder aux données chiffrées. Dans le chiffrement asymétrique, la clé privée doit être stockée en lieu sûr, car elle est utilisée pour déchiffrer les données.

SEC-LEC : Durcissement sécurité Linux

Protection des fichiers - Le chiffrement des fichiers

Sous Linux, il existe de nombreuses options pour chiffrer des fichiers.

Voici quelques méthodes courantes :

- **Chiffrement de fichiers avec GnuPG (GPG)** : GPG est un outil open source qui utilise des algorithmes de chiffrement asymétriques pour chiffrer des fichiers. Pour chiffrer un fichier avec GPG, vous devez d'abord générer une paire de clés (une clé publique et une clé privée), puis utiliser la clé publique pour chiffrer le fichier. Seule la personne qui possède la clé privée peut déchiffrer le fichier.
- **Chiffrement de fichiers avec OpenSSL** : OpenSSL est une bibliothèque open source qui prend en charge les algorithmes de chiffrement symétriques et asymétriques. Pour chiffrer un fichier avec OpenSSL, vous pouvez utiliser l'outil openssl enc en spécifiant l'algorithme de chiffrement et la clé de chiffrement. Vous pouvez également utiliser OpenSSL pour chiffrer des fichiers avec des certificats X.509.
- **Chiffrement de fichiers avec EncFS** : EncFS est un outil open source qui crée un système de fichiers chiffré en utilisant des algorithmes de chiffrement symétriques. Pour utiliser EncFS, vous devez d'abord créer un dossier chiffré et un dossier monté, puis utiliser EncFS pour monter le dossier chiffré sur le dossier monté. Tout ce qui est stocké dans le dossier monté est automatiquement chiffré et déchiffré lorsque vous y accédez.
- **Chiffrement de fichiers avec VeraCrypt** : VeraCrypt est un outil open source pour créer des volumes chiffrés, qui peuvent être utilisés pour stocker des fichiers chiffrés. Vous pouvez créer un volume chiffré et le monter sur votre système de fichiers en utilisant VeraCrypt, puis ajouter ou supprimer des fichiers de ce volume chiffré comme s'il s'agissait d'un dossier normal.
- **Chiffrement de fichiers avec dm-crypt/LUKS** : dm-crypt est un outil de chiffrement de disque complet pour Linux. LUKS (Linux Unified Key Setup) est une spécification pour la gestion des clés de chiffrement pour les volumes chiffrés avec dm-crypt. Vous pouvez créer un volume chiffré avec dm-crypt/LUKS et le monter sur votre système de fichiers comme un disque normal. Tout ce qui est stocké sur ce disque sera automatiquement chiffré et déchiffré lorsque vous y accédez.

Il est important de noter que la sécurité d'un système de chiffrement dépend de la qualité de la clé de chiffrement utilisée et de la sécurité de la gestion de cette clé. Il est également important de sauvegarder la clé de chiffrement en lieu sûr pour éviter de perdre l'accès aux fichiers chiffrés.

SEC-LEC : Durcissement sécurité Linux

Protection des fichiers - Le chiffrement des fichiers

Créer une partition chiffrée dans un fichier à l'aide de VeraCrypt :

- Tout d'abord, **téléchargez et installez VeraCrypt** depuis le site officiel : https://www.veracrypt.fr
- Lancez VeraCrypt et cliquez sur le bouton "Créer un volume" dans la fenêtre principale
- Dans la fenêtre "Assistant Volume de VeraCrypt", choisissez "Créer un volume chiffré dans un fichier" et cliquez sur "Suivant"
- Sélectionnez "Sélectionner un fichier" et cliquez sur "Parcourir" pour choisir un emplacement et un nom de fichier pour votre partition chiffrée. Assurez-vous que le fichier est de taille suffisante pour contenir la partition que vous souhaitez créer
- Dans la fenêtre suivante, choisissez l'algorithme de chiffrement et le mode de hachage que vous souhaitez utiliser pour chiffrer le fichier. Si vous n'êtes pas sûr de ce qu'il faut choisir, les options par défaut devraient être suffisantes.
- Entrez la taille de la partition chiffrée que vous souhaitez créer. Vous pouvez choisir une taille en bytes, kilobytes, megabytes, ou gigabytes.
- Entrez un mot de passe fort pour votre partition chiffrée et cliquez sur "Suivant".
- Dans la fenêtre suivante, choisissez un système de fichiers pour votre partition chiffrée. Encore une fois, si vous n'êtes pas sûr de ce qu'il faut choisir, les options par défaut devraient être suffisantes.
- Cliquez sur "Générer" pour créer une clé de chiffrement pour votre partition chiffrée. Vous pouvez enregistrer cette clé sur un support externe si vous le souhaitez.
- Dans la dernière fenêtre de l'assistant, cliquez sur "Terminer" pour créer votre partition chiffrée. La partition sera créée dans le fichier que vous avez spécifié à l'étape 4.
- Pour monter la partition chiffrée, lancez VeraCrypt et cliquez sur "Sélectionner un fichier" dans la fenêtre principale. Choisissez le fichier dans lequel vous avez créé la partition chiffrée et cliquez sur "Ouvrir".
- Cliquez sur "Monter" pour monter la partition chiffrée. Vous devrez entrer le mot de passe que vous avez créé à l'étape 7.
- La partition chiffrée apparaîtra maintenant dans l'explorateur de fichiers de votre système d'exploitation, et vous pourrez y accéder comme à une partition normale.

Voilà, vous avez maintenant créé une partition chiffrée dans un fichier avec VeraCrypt !

N'oubliez pas de démonter la partition chiffrée lorsque vous n'en avez plus besoin, afin de protéger vos données en cas de vol ou de perte de votre ordinateur.

SEC-LEC : Durcissement sécurité Linux

Protection des fichiers - Le chiffrement des fichiers

Pour créer une paire de clés GPG sur Linux, vous pouvez suivre les étapes suivantes :

- Installez GPG si ce n'est pas déjà fait sur votre système. Sur Ubuntu et d'autres distributions basées sur Debian, vous pouvez utiliser la commande suivante dans un terminal :

  sudo apt install gnupg

- Ouvrez un terminal et tapez la commande suivante :

  gpg --full-generate-key

- Suivez les instructions à l'écran pour configurer votre paire de clés. Vous serez invité à fournir les informations suivantes :

* Le type de clé que vous souhaitez générer (RSA ou DSA)
* La taille de la clé que vous souhaitez générer (2048 bits est une bonne taille pour la plupart des utilisateurs)
* La durée de validité de la clé (la valeur par défaut est 2 ans)
* Votre nom complet
* Votre adresse email
* Un commentaire (facultatif)
* Un mot de passe pour protéger la clé privée (assurez-vous de choisir un mot de passe fort et de le conserver en sécurité)

Une fois que vous avez fourni toutes les informations, la commande générera une paire de clés publique/privée et les stockera sur votre système.

- Vous pouvez afficher les détails de votre clé publique en utilisant la commande suivante :

  gpg --list-keys

- Et pour afficher les détails de votre clé privée, vous pouvez utiliser la commande suivante :

  gpg --list-secret-keys

Il est important de sauvegarder votre clé privée en lieu sûr et de ne pas la divulguer à d'autres personnes. La sécurité de votre paire de clés GPG dépend de la qualité de votre mot de passe et de la sécurité de la gestion de votre clé privée.

Protection des fichiers - Le chiffrement des fichiers

➡ Voici un exemple de commande pour chiffrer un fichier avec GPG sur Linux :

gpg --output fichier_chiffre.gpg --encrypt --recipient destinataire fichier_original

Dans cette commande, "fichier_original" est le nom du fichier que vous souhaitez chiffrer et "destinataire" est le nom ou l'adresse email de la personne à qui vous souhaitez envoyer le fichier chiffré. GPG utilisera la clé publique de cette personne pour chiffrer le fichier.

Une fois que vous avez chiffré le fichier, vous pouvez l'envoyer par email ou tout autre moyen de transmission de fichier.

La personne qui reçoit le fichier chiffré doit disposer de la clé privée correspondant à la clé publique utilisée pour chiffrer le fichier afin de le déchiffrer.

➡ Voici un exemple de commande pour déchiffrer un fichier chiffré avec GPG :

gpg --output fichier_original --decrypt fichier_chiffre.gpg

Dans cette commande, "fichier_chiffre.gpg" est le nom du fichier chiffré que vous souhaitez déchiffrer et "fichier_original" est le nom que vous souhaitez donner au fichier déchiffré.

Des Questions

SEC-LEC : Durcissement sécurité Linux
La sécurité du noyau

SEC-LEC : Durcissement sécurité Linux

La sécurité du noyau - Sysctl

sysctl est une commande utilisée sur les systèmes d'exploitation basés sur Unix tels que Linux, macOS ou FreeBSD, permettant de modifier ou afficher les paramètres de configuration du noyau du système d'exploitation.

/etc/sysctl.d est un répertoire présent sur certaines distributions Linux, contenant des fichiers de configuration *.conf pour sysctl. Ces fichiers contiennent des paramètres de configuration qui sont chargés lors du démarrage du système, afin de personnaliser le comportement du système d'exploitation. Les fichiers peuvent être créés par les administrateurs système pour modifier les paramètres de configuration du système, tels que les limites de la mémoire, les paramètres réseau, les informations sur le matériel, et d'autres options de configuration du système.

L'utilisation de /etc/sysctl.d permet de simplifier la gestion des paramètres de configuration du système, en permettant de les organiser en fichiers distincts, plutôt que de les placer dans un seul fichier de configuration. Cela facilite également la gestion des changements de configuration, car il est plus facile de trouver et de modifier des paramètres spécifiques dans des fichiers séparés.

SEC-LEC : Durcissement sécurité Linux

La sécurité du noyau - Sysctl

Voici quelques exemples de commandes sysctl spécifiques à Ubuntu avec une brève explication de leur fonction :

- Afficher tous les paramètres de configuration disponibles : *sysctl -a*
- Afficher les paramètres de configuration de la mémoire virtuelle (default 60) :
  sysctl vm.swappiness
- Activer l'envoi de messages de débogage au noyau (max 8) :
  sysctl kernel.printk=8
- Limiter le nombre maximum de processus :
  sysctl kernel.pid_max=65536
- Désactiver l'exécution de code sur des partitions montées en mode noexec :
  sysctl fs.protected_hardlinks=1
- Limiter la taille maximale des messages système :
  sysctl kernel.msgmax=65536
- Augmenter le nombre maximum de connexions simultanées :
  sysctl net.core.somaxconn=4096

SEC-LEC : Durcissement sécurité Linux

La sécurité du noyau - /proc/sys

/proc/sys est un système de fichiers virtuel dans les systèmes d'exploitation Linux qui permet d'accéder et de modifier des paramètres du noyau en temps réel. Chaque fichier dans /proc/sys représente une variable de configuration système différente, telle que le nombre maximum de fichiers ouverts, la taille maximale de la pile, etc.

sysctl, quant à lui, est une commande utilisée pour interagir avec le système de paramètres du noyau Linux.

En utilisant sysctl, les utilisateurs peuvent modifier les valeurs des variables de configuration système stockées dans /proc/sys, ainsi que récupérer des informations sur les variables de configuration système actuelles.

En d'autres termes, sysctl est un outil en ligne de commande utilisé pour interagir avec les variables de configuration système stockées dans le système de fichiers virtuel /proc/sys. Les modifications apportées aux paramètres du noyau à l'aide de la commande sysctl se reflètent immédiatement dans les fichiers correspondants dans /proc/sys.

SEC-LEC : Durcissement sécurité Linux

La sécurité du noyau - Linux Security Modules (LSM)

Le modèle de contrôle d'accès standard Unix, également appelé modèle de **contrôle d'accès discrétionnaire (DAC)**, est un modèle de sécurité dans lequel les propriétaires de fichiers peuvent contrôler l'accès à leurs fichiers en définissant les permissions d'accès sur ces fichiers. Dans le modèle DAC, chaque utilisateur possède un identifiant de groupe et un ensemble de permissions d'accès (lecture, écriture et exécution) pour chaque fichier. Le propriétaire du fichier peut accorder ou refuser l'accès à un fichier en fonction de ces autorisations.

À l'inverse, les modèles de **contrôle d'accès obligatoires (MAC)** sont des modèles de sécurité qui permettent au système d'imposer des règles de sécurité pour chaque objet sur la base d'une politique de sécurité définie. Dans le modèle MAC, les autorisations sont déterminées en fonction d'un ensemble de règles de sécurité qui sont définies par l'administrateur système ou un organisme de sécurité. Les politiques MAC permettent un contrôle plus fin de l'accès aux fichiers et aux ressources système, ce qui peut aider à protéger les systèmes contre des attaques telles que les attaques par dépassement de tampon ou l'exécution de code malveillant.

Les LSM implémentent le modèle MAC dans linux.

SEC-LEC : Durcissement sécurité Linux

La sécurité du noyau - Linux Security Modules (LSM)

Les **Linux Security Modules (LSM)** sont un framework de sécurité du noyau Linux qui fournit une interface générique pour la mise en place de mécanismes de sécurité supplémentaires au-delà des mécanismes de sécurité de base fournis par le noyau Linux.

Les LSM sont utilisés pour étendre les capacités de sécurité du noyau, tels que les contrôles d'accès obligatoires, les vérifications de sécurité d'intégrité des fichiers, les mécanismes de confinement de processus, et bien plus encore.

LSM fournit une API pour permettre aux différents modules de sécurité d'enregistrer des points d'accès dans le noyau et de contrôler le comportement du noyau. Enregistrer ces points d'accès permet à chaque module de sécurité de contrôler la façon dont les opérations spécifiques du noyau sont effectuées. Les différents modules de sécurité peuvent fournir des politiques de sécurité personnalisées, des restrictions d'accès pour des utilisateurs spécifiques, et des mécanismes pour détecter et prévenir des attaques.

Certains exemples de LSM populaires sont **SELinux (Security Enhanced Linux), AppArmor, et Smack**. Les administrateurs système peuvent choisir d'activer l'un de ces modules de sécurité pour ajouter des couches supplémentaires de sécurité au système Linux.

SEC-LEC : Durcissement sécurité Linux

La sécurité du noyau - Linux Security Modules (LSM)

Voici une liste des LSM (Linux Security Modules) les plus couramment utilisés sur les systèmes Linux :

- **SELinux** (Security-Enhanced Linux) : développé par la NSA (National Security Agency), SELinux est un module de sécurité qui offre une sécurité renforcée pour les systèmes Linux en utilisant des politiques de sécurité basées sur les contrôles obligatoires d'accès.
- **AppArmor** : un module de sécurité qui fournit des politiques de sécurité basées sur les profils d'application, qui permettent de limiter les actions qu'une application peut effectuer sur un système.
- **Smack** (Simplified Mandatory Access Control Kernel) : un module de sécurité qui fournit un contrôle d'accès obligatoire simplifié pour les fichiers et les processus sur un système Linux.
- **Tomoyo** : un module de sécurité qui fournit des politiques de sécurité basées sur les politiques d'utilisation de ressources pour contrôler l'accès aux fichiers et processus sur un système.
- **Yama** (Yet Another Mandatory Access control) : un module de sécurité qui fournit des politiques de sécurité pour les processus qui sont exécutés avec des privilèges élevés.

Ces modules de sécurité sont souvent utilisés en combinaison avec d'autres outils de sécurité tels que les pare-feux, les outils de surveillance, les outils de détection de vulnérabilités, etc., pour renforcer la sécurité des systèmes Linux.

SEC-LEC : Durcissement sécurité Linux

La sécurité du noyau - LSM - SELinux

SELinux (Security-Enhanced Linux) est un module de sécurité du noyau Linux qui implémente le modèle de contrôle d'accès obligatoire (MAC). Développé à l'origine par la National Security Agency (NSA) des États-Unis, SELinux est désormais un projet open source communautaire.

Le modèle de sécurité de SELinux étend le modèle de contrôle d'accès standard Unix (DAC) en ajoutant une politique de sécurité qui définit les règles de contrôle d'accès pour chaque objet dans le système (fichiers, processus, ports réseau, etc.). Cette politique de sécurité est contrôlée par des administrateurs système et est généralement basée sur les règles de sécurité de type "contrôle d'accès obligatoire" (MAC). Cette politique permet à SELinux de restreindre l'accès des processus aux ressources système, limitant ainsi l'impact des vulnérabilités de sécurité potentielles.

SELinux fonctionne en ajoutant une couche de contrôle d'accès à chaque objet du système. Lorsqu'un processus demande l'accès à un objet, SELinux consulte la politique de sécurité pour déterminer si l'accès doit être autorisé. Si la demande d'accès est autorisée, SELinux ajoute une étiquette de sécurité au processus qui indique quelles opérations sont autorisées pour ce processus.

Bien que SELinux offre un niveau de sécurité supplémentaire, il peut être difficile à configurer et peut entrer en conflit avec des applications tierces. Cependant, de nombreux systèmes Linux modernes incluent SELinux par défaut, et les administrateurs système peuvent travailler avec les développeurs d'applications pour garantir que les applications sont compatibles avec SELinux.

La sécurité du noyau - LSM - SELinux

Voici une explication des commandes standard de SELinux :

- **Le paramètre -Z** : Le paramètre -Z est utilisé pour afficher ou modifier l'étiquette de sécurité d'un fichier ou d'un répertoire. Par exemple, la commande "*ls -Z*" affichera l'étiquette de sécurité de chaque fichier dans le répertoire courant.
- **selinux-activate** : La commande selinux-activate est utilisée pour activer SELinux sur un système qui n'utilise pas SELinux par défaut. Cette commande peut être utilisée pour activer SELinux sans redémarrer le système.
- **sestatus** : La commande sestatus est utilisée pour afficher l'état actuel de SELinux sur le système. Elle affiche les informations sur la politique de sécurité actuellement en cours d'utilisation, ainsi que les modes SELinux actuellement activés sur le système.
- **getenforce** : La commande getenforce est utilisée pour afficher le mode SELinux actuellement activé sur le système. Elle peut afficher "**Enforcing**" si SELinux est activé, ou "**Permissive**" si SELinux est activé en mode permissif.
- **setenforce** : La commande setenforce est utilisée pour activer ou désactiver le mode SELinux sur le système. Elle peut être utilisée pour passer de "Enforcing" à "Permissive" ou vice versa.
- **/etc/selinux/config** : Le fichier /etc/selinux/config est utilisé pour configurer SELinux sur le système. Il contient les paramètres de configuration SELinux, tels que le mode d'activation de SELinux, la politique de sécurité en cours d'utilisation et les paramètres de journalisation SELinux.

Ces commandes sont souvent utilisées pour gérer SELinux sur un système Linux et pour diagnostiquer les problèmes de sécurité.

La sécurité du noyau - LSM - SELinux

Pour installer SELinux sur Ubuntu, vous pouvez suivre les étapes suivantes :

- Ouvrez un terminal et exécutez la commande suivante pour installer les packages nécessaires :
  sudo apt install selinux-policy-default selinux-utils selinux-basics
- Redémarrez votre système pour activer SELinux
- Vérifiez que SELinux est activé en exécutant la commande suivante : *sestatus*
- Si SELinux est activé, vous devriez voir une sortie similaire à la suivante :
  SELinux status: enabled
  SELinuxfs mount: /sys/fs/selinux
  SELinux root directory: /etc/selinux
  Loaded policy name: default
  Current mode: enforcing
  Mode from config file: enforcing
  Policy MLS status: enabled
  Policy deny_unknown status: allowed
  Max kernel policy version: 31
- Maintenant que SELinux est installé et activé, vous pouvez tester la commande ls -Z /etc/passwd pour voir les attributs de sécurité SELinux pour le fichier /etc/passwd.

La commande ls -Z affiche les attributs de sécurité SELinux pour les fichiers et répertoires. La sortie devrait ressembler à quelque chose comme ceci :

-rw-r--r--. root root system_u:object_r:etc_t:s0 /etc/passwd

Le libellé system_u:object_r:etc_t:s0 indique le contexte de sécurité SELinux pour le fichier. Dans ce cas, etc_t est le type de fichier SELinux pour /etc/passwd. Le contexte de sécurité SELinux est utilisé pour déterminer les autorisations de sécurité pour un fichier ou un processus.

GrSecurity

Il y a problème avec grSecurity, Il est devenu payant.

Il est donc impossible de le présenter ici.

SEC-LEC : Durcissement sécurité Linux

La sécurité du noyau - LSM - AppArmor

AppArmor est un framework de sécurité pour Linux qui permet de limiter les actions qu'un processus peut effectuer en se basant sur des règles de sécurité prédéfinies. AppArmor est utilisé pour limiter les dommages potentiels causés par les vulnérabilités de sécurité ou les erreurs de configuration d'une application ou d'un système. Il est similaire à SELinux, un autre framework de sécurité pour Linux, mais avec des différences significatives dans la façon dont il gère les politiques de sécurité.

L'un des avantages d'AppArmor est qu'il est relativement facile à configurer et à utiliser. Il utilise des profils de sécurité prédéfinis pour de nombreuses applications courantes, ce qui facilite l'application de politiques de sécurité à ces applications sans avoir à écrire de règles personnalisées.

Les profils de sécurité AppArmor peuvent être configurés pour spécifier les fichiers et les ressources système auxquels un processus est autorisé à accéder, ainsi que les opérations qu'il est autorisé à effectuer sur ces ressources. Les profils de sécurité peuvent être configurés pour les applications système, les services système et les applications tierces. Les profils peuvent également être configurés pour les processus système tels que les démons et les services.

En résumé, AppArmor est un framework de sécurité flexible et facile à utiliser pour Linux qui permet de limiter les actions qu'un processus peut effectuer en se basant sur des règles de sécurité prédéfinies. Il offre des profils de sécurité pour de nombreuses applications courantes, mais permet également la configuration de politiques de sécurité personnalisées pour les applications tierces et les processus système.

SEC-LEC : Durcissement sécurité Linux

La sécurité du noyau - LSM - AppArmor

Le paquet apparmor-utils est un ensemble d'utilitaires qui permettent de gérer AppArmor, un framework de sécurité pour Linux.

Voici une présentation des commandes de apparmor disponibles dans le paquet apparmor-utils :

- **apparmor_status** : Cette commande affiche le statut actuel de AppArmor et les profils de sécurité activés pour les processus en cours d'exécution. La commande affiche également les processus qui ont été confinés par AppArmor et les profils de sécurité qui sont en mode "complain" ou "enforce". Elle permet donc de vérifier l'état de la sécurité des processus de votre système.
- **aa_enforce** : Cette commande permet de basculer un profil de sécurité AppArmor en mode "enforce", ce qui signifie que les processus associés à ce profil seront restreints par les règles de sécurité AppArmor. Cette commande permet de forcer l'application de règles de sécurité pour un profil donné.
- **aa_complain** : Cette commande permet de basculer un profil de sécurité AppArmor en mode "complain", ce qui signifie que les processus associés à ce profil ne seront pas restreints par les règles de sécurité AppArmor, mais que les violations seront enregistrées dans les logs. Cette commande permet de tester un profil de sécurité sans restreindre réellement les processus associés.
- **apparmor_parser** : Cette commande permet de vérifier la syntaxe d'un profil de sécurité AppArmor et de le compiler en un format utilisable par le noyau Linux. Elle est utilisée pour valider et compiler les règles de sécurité définies pour les profils.

En utilisant ces commandes, vous pouvez configurer, gérer et vérifier la sécurité de votre système Linux avec AppArmor.

La sécurité du noyau - LSM - AppArmor

Le répertoire /etc/apparmor.d est l'emplacement où les fichiers de configuration des profils de sécurité AppArmor sont stockés. Ce répertoire contient les fichiers de configuration pour les profils de sécurité système et pour les applications tierces qui ont des profils de sécurité AppArmor définis.

Les fichiers de configuration dans le répertoire /etc/apparmor.d sont au format texte et sont utilisés pour définir les règles de sécurité pour les profils AppArmor. Ces fichiers sont organisés par nom de profil de sécurité, et chaque fichier contient des règles qui spécifient les ressources système auxquelles un processus est autorisé à accéder et les opérations qu'il est autorisé à effectuer sur ces ressources.

Les paquets apparmor-profiles* sont un ensemble de profils de sécurité prédéfinis pour des applications courantes. Ces profils de sécurité sont inclus dans les distributions Linux qui prennent en charge AppArmor, telle que Ubuntu. Les profils de sécurité peuvent être installés en installant le paquet apparmor-profiles, qui inclut des profils pour des applications telles que Apache, MySQL, Nginx, etc.

Le paquet apparmor-profiles est divisé en sous-paquets pour différentes catégories d'applications, tels que apparmor-profiles-extra et apparmor-profiles-ubuntu-core. Les sous-paquets sont installés séparément, selon les besoins de l'utilisateur.

SEC-LEC : Durcissement sécurité Linux

La sécurité du noyau - LSM - AppArmor

Voici une description ligne à ligne du fichier **/etc/apparmor.d/bin.ping** :

# Last Modified: Tue Sep 28 17:28:13 2021	
2. #include <tunables/global>	Cette ligne inclut le fichier global des réglages de tunables.
3.	
4. profile bin.ping flags=(attach_disconnected,mediate_deleted) {	Cette ligne définit le profil de sécurité pour l'exécutable ping. Les drapeaux attach_disconnected et mediate_deleted indiquent que les processus attachés et les processus supprimés seront gérés par AppArmor.
5. #include <abstractions/base>	Cette ligne inclut le fichier base des abstractions AppArmor.
6.	
7. capability net_raw,	Cette ligne autorise la capacité net_raw
8. capability setuid,	Cette ligne autorise la capacité setuid.
9. capability setgid,	Cette ligne autorise la capacité setgid
10.	
11. /bin/ping mr,	Cette ligne autorise l'accès en lecture et en écriture à l'exécutable /bin/ping avec le mode d'accès mr, qui signifie que le fichier ne peut être ouvert qu'en lecture.
12. /etc/host.conf r,	Cette ligne autorise l'accès en lecture au fichier /etc/host.conf.
13. /etc/hosts r,	Cette ligne autorise l'accès en lecture au fichier /etc/hosts.
14. /etc/nsswitch.conf r,	Cette ligne autorise l'accès en lecture au fichier /etc/nsswitch.conf.
15. /etc/resolv.conf r,	Cette ligne autorise l'accès en lecture au fichier /etc/resolv.conf.
16. /usr/share/locale/** r,	Cette ligne autorise l'accès en lecture à tous les fichiers dans le répertoire /usr/share/locale/ et ses sous-répertoires.
17. }	

En résumé, le fichier /etc/apparmor.d/bin.ping définit les règles de sécurité pour l'exécutable ping. Les règles incluent l'autorisation des capacités net_raw, setuid et setgid, ainsi que l'autorisation de l'accès en lecture à plusieurs fichiers système, notamment les fichiers de configuration réseau.

Des Questions

SEC-LEC : Durcissement sécurité Linux
Les malwares sous Linux

SEC-LEC : Durcissement sécurité Linux

Les malwares sous Linux

Les malwares sous Linux sont relativement rares en comparaison avec les systèmes Windows, principalement en raison des différences architecturales entre les deux systèmes d'exploitation et de la part de marché plus faible de Linux sur les ordinateurs personnels. Cependant, cela ne signifie pas que les malwares sur Linux n'existent pas ou qu'ils ne sont pas dangereux. Les attaquants ciblent souvent les serveurs Linux, qui sont largement utilisés dans les data centers et sur Internet, en raison de leur fiabilité, de leur flexibilité et de leur performance.

Les malwares sous Linux peuvent avoir des impacts similaires à ceux sur Windows, tels que la perte de données, l'usurpation d'identité, l'extorsion, etc. Cependant, ils sont souvent plus ciblés et sophistiqués, et sont souvent associés à des attaques avancées menées par des groupes de cybercriminels ou des États-nations.

En termes de nombre de malwares, il est difficile de donner une estimation précise car les malwares évoluent rapidement et les nouveaux malwares sont découverts tous les jours. Cependant, selon les rapports de sécurité, les malwares sous Linux représentent une petite fraction du total des malwares détectés, par rapport aux malwares sur Windows.

En ce qui concerne la criticité, les malwares sous Linux peuvent avoir un impact très important sur les entreprises et les organisations, en particulier celles qui dépendent fortement des technologies de l'information et de la communication. Les serveurs Linux hébergent souvent des applications web critiques, des bases de données et des services de messagerie, et leur compromission peut entraîner des pertes financières importantes, une violation de la vie privée des utilisateurs et une atteinte à la réputation de l'entreprise.

En comparaison, les malwares sur Windows sont souvent plus répandus et moins ciblés, mais peuvent être très nuisibles pour les utilisateurs individuels et les entreprises. Les malwares Windows sont souvent associés à des campagnes de spam, des escroqueries en ligne, des botnets et des logiciels espions.

Les malwares sous Linux - Les types de malwares sous Linux

Une liste de certains types de malwares qui ont été découverts sur des systèmes Linux :

- **Les chevaux de Troie (Trojan)** : ces malwares se font passer pour des programmes légitimes afin de tromper l'utilisateur et de se propager sur le système. Un exemple est le malware Linux.Rex.1, qui a été découvert en 2016 et qui permet à un attaquant de prendre le contrôle à distance du système infecté.
- **Les vers (Worm)** : ces malwares se propagent automatiquement à travers un réseau en exploitant des vulnérabilités. Un exemple est le ver Linux.Darlloz, qui a été découvert en 2014 et qui se propageait en exploitant une vulnérabilité dans le firmware des routeurs.
- **Les rançongiciels (Ransomware)** : ces malwares chiffrent les fichiers de l'utilisateur et exigent une rançon en échange de la clé de déchiffrement. Un exemple est le rançongiciel Linux.Encoder.1, qui a été découvert en 2015 et qui a ciblé des serveurs Web Linux.
- **Les rootkits** : ces malwares sont conçus pour cacher leur présence sur le système en modifiant le comportement du système d'exploitation. Un exemple est le rootkit Linux.Snake, qui a été découvert en 2014 et qui se cachait en modifiant des fichiers système critiques.
- **Les backdoors** : ces malwares créent une porte dérobée sur le système, permettant à un attaquant de prendre le contrôle du système à distance. Un exemple est le backdoor Linux.Hoflack, qui a été découvert en 2014 et qui permet à un attaquant de prendre le contrôle à distance du système infecté.

Il est important de noter que les malwares sur Linux sont relativement rares par rapport à d'autres systèmes d'exploitation, mais cela ne signifie pas qu'il ne faut pas prendre de mesures de sécurité pour les prévenir.

Les malwares sous Linux

Simulation d'attaque

Dans le fichier **bindshell**, je montre comment traiter une suspicion d'attaque bind shell.

Nous allons simuler une attaque bindshell sur notre linux.

On utilise netcat pour ce faire.

```
cd /tmp
cp /bin/nc /tmp/freedom
./freedom -k -w 1 -l 41000 > /dev/null &
rm freedom
```

On efface le fichier nc copié dans /tmp après usage, pour montre comment on peut le récupérer.

```
ss /nalp
```

montre un process 'freedom' inconnu avec un port ouvert.

```
ls -al /proc/PID (PID obtenu à la commande précédente)
```

....

SEC-LEC : Durcissement sécurité Linux

Les malwares sous Linux - Les rootkits

Les rootkits sont des outils malveillants qui sont utilisés pour accéder à un système d'exploitation sans autorisation et obtenir un contrôle total.

Sous Linux, les rootkits sont généralement implémentés sous forme de binaires qui peuvent être exécutés à partir d'une ligne de commande et modifient le noyau Linux pour prendre le contrôle des processus système et des fonctions système, y compris le système de fichiers et le système réseau.

Les rootkits peuvent également être utilisés pour modifier les fonctions de sécurité du système d'exploitation, ce qui permet aux attaquants d'accéder à des informations sensibles et d'effectuer des actions non autorisées.

Les rootkits sous Linux sont généralement cachés dans des répertoires, des binaires ou des fichiers cachés et ne laissent aucune trace de leur présence et de leurs activités sur le système.

Il est donc important que les administrateurs système utilisent des outils de sécurité pour détecter les rootkits et les supprimer avant qu'ils ne causent des dommages.

Les malwares sous Linux - Les rootkits

Sous linux, deux outils sont connus pour faire la chasse aux rootkits.

- chkrootkit : Shell script qui teste localement des signes de présence de rootkit en comparaison d'une liste de comportement de rootkit connus
- rkhunter : Utilise Unhide pour comparer une base en ligne des traces des rootkits connus avec le contenu de votre ordinateur pour y détecter les indices de compromission

SEC-LEC : Durcissement sécurité Linux

Les malwares sous Linux - Les rootkits

Description de deux anti-rootkit :

- chkrootkit : Outil open source qui permet aux utilisateurs de détecter les logiciels malveillants sur leurs systèmes. Il est capable de rechercher des exploits connus, des backdoors et des « rootkits » cachés sur le système. Chkrootkit s'exécute automatiquement et recherche des programmes malveillants dans plusieurs répertoires et fichiers, et peut également rechercher des fichiers cachés. Il est facile à installer, configurer et utiliser, et est disponible pour diverses plates-formes, y compris Linux et Mac OS X. Chkrootkit est un outil utile pour les utilisateurs qui souhaitent surveiller leur système et déterminer s'il y a des logiciels malveillants présents, et permet de prévenir potentiellement les attaques de logiciels malveillants avant qu'elles ne puissent causer des dommages.
- Installation : sudo apt install chkrootkit
- Utilisation : sudo /usr/sbin/chkrootkit
- Résultat :

```
ROOTDIR is `/'
Checking `amd'...                                           not found
Checking `basename'...                                      not infected
Checking `biff'...                                          not found
Checking `chfn'...                                          not infected
Checking `chsh'...                                          not infected
Checking `cron'...                                          not infected
Checking `crontab'...                                       not infected
Checking `date'...                                          not infected
Checking `du'...                                            not infected
Checking `dirname'...                                       not infected
Checking `echo'...                                          not infected
Checking `egrep'...                                         not infected
...
```

Les malwares sous Linux - Les rootkits

- rkhunter : Outil de détection de logiciels malveillants open source qui peut être utilisé avec le système d'exploitation Linux. Il vérifie les fichiers système, les configurations et les installations de logiciels et recherche des modifications inhabituelles qui peuvent être le signe d'une activité malveillante. L'outil compare également les fichiers système à une base de données de signatures de logiciels malveillants connus et peut prendre des mesures pour bloquer l'accès aux fichiers suspects. RKHunter se démarque en ce qu'il peut être utilisé pour surveiller les changements dans le système d'exploitation et les logiciels installés ainsi que les tentatives d'accès non autorisées. Il fournit également un tableau de bord pour l'administrateur système qui offre des informations sur l'état de sécurité actuelle et peut aider les utilisateurs à détecter et à corriger les problèmes rapidement et efficacement.
- Installation : *sudo apt install rkhunter*
- Mise à jour : *sudo rkhunter --update*
- liste des tests disponibles : *sudo rkhunter --list*
- Vérification : *sudo rkhunter --checkall*
- Version plus sûre : *sudo rkhunter -c --rwo*

Les malwares sous Linux - Solutions anti-malwares

clamav : ClamAV est une boîte à outils antivirus open source (GPLv2), conçue spécialement pour l'analyse des e-mails sur les passerelles de messagerie. Il fournit un certain nombre d'utilitaires, notamment un démon multithread flexible et évolutif, un scanner en ligne de commande et un outil avancé de mise à jour automatique de la base de données. Le cœur du paquet est un moteur anti-virus disponible sous forme de bibliothèque partagée.

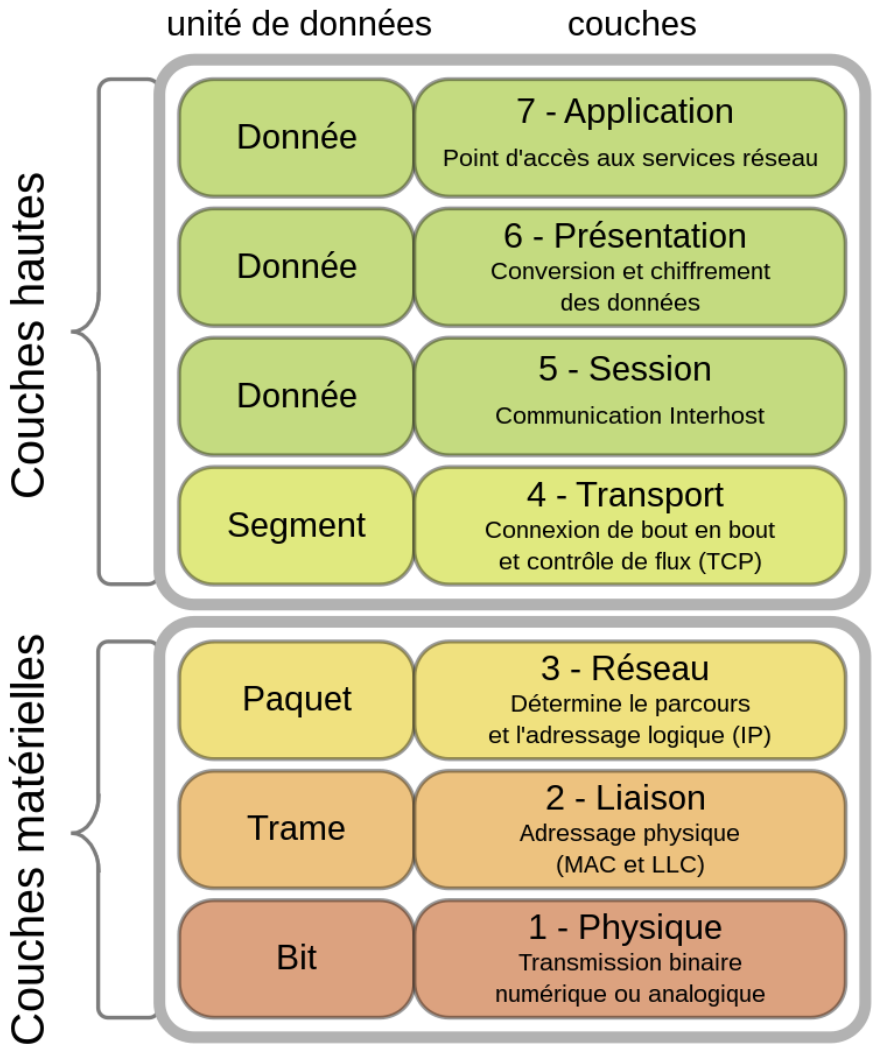
- Installation : *sudo apt install clamav*
- Check : *sudo clamscan --version*
- Mise a jour de la base de données : *sudo freshclam*
- Check de son homedir : *sudo clamscan --infected --remove --recursive ~/*

La sécurité du réseau - Modèle OSI : rappel

Le modèle OSI (Open Systems Interconnection) est un modèle de référence pour les réseaux informatiques. Il a été développé par l'ISO (International Organization for Standardization) pour faciliter la communication entre différents systèmes informatiques.

Le modèle OSI se compose de sept couches, chacune ayant un rôle spécifique dans la communication des données. Les sept couches sont :

- **physique** : Cette couche est responsable de la transmission de bits bruts sur le support de communication, tels que les câbles Ethernet ou les ondes radio
- **liaison de données** : Cette couche est responsable de la transmission des données de la couche physique entre des nœuds adjacents sur le réseau, en s'assurant que les données sont transmises sans erreur
- **réseau** : Cette couche est responsable de la transmission de paquets de données sur le réseau, en utilisant des protocoles de routage pour acheminer les données entre les différents réseaux



La sécurité du réseau - Modèle OSI : rappel

Il reste quatre couches :

- **transport** : Cette couche est responsable de la gestion de la transmission des données entre les applications en utilisant des protocoles tels que TCP (Transmission Control Protocol) ou UDP (User Datagram Protocol)
- **Session** : Cette couche est responsable de l'établissement, le maintien et la fin de la connexion entre les applications sur différents nœuds du réseau
- **Présentation** : Cette couche est responsable de la conversion des données dans un format compréhensible par l'application, en s'assurant que les différents systèmes sont compatibles
- **Application** : Cette couche est responsable de la communication entre les applications elles-mêmes, telles que les navigateurs Web ou les clients de messagerie électronique

En suivant le modèle OSI, les développeurs de réseaux peuvent s'assurer que les différents systèmes informatiques sont compatibles et peuvent communiquer efficacement entre eux.

La sécurité du réseau - Panorama des attaques

Voici quelques-unes des attaques courantes au niveau des protocoles :

- **Attaques d'interception** : Les attaquants peuvent utiliser des outils tels que des sniffeurs de paquets pour intercepter les données qui circulent sur le réseau, y compris les informations d'identification et les données sensibles.
- **Attaques de rejeu** : Les attaquants peuvent enregistrer les échanges de données entre les parties et les rejouer plus tard pour tromper les systèmes de sécurité ou les utilisateurs légitimes.
- **Attaques d'injection de données** : Les attaquants peuvent injecter des données malveillantes dans les échanges de données pour exploiter les vulnérabilités des systèmes ou exécuter des codes malveillants sur les ordinateurs cibles.
- **Attaques de falsification d'adresse IP** : Les attaquants peuvent utiliser des techniques de falsification d'adresse IP pour masquer leur identité et accéder aux systèmes ou aux réseaux sans autorisation.

La sécurité du réseau - Sécurité au niveau de la couche physique

La couche 1 du modèle OSI, également appelée couche physique, est responsable de la transmission des bits bruts sur le support de communication. Cette couche est souvent considérée comme la plus vulnérable en termes de sécurité, car elle est directement accessible aux attaquants physiques qui ont un accès physique au réseau.

Voici quelques faiblesses de sécurité spécifiques de la couche 1 OSI :

- **Espionnage** : Les attaquants peuvent intercepter les signaux électriques ou optiques transmis sur le support de communication pour accéder aux informations confidentielles
- **Interférences électromagnétiques** : Les signaux électromagnétiques peuvent être perturbés par des sources électromagnétiques externes, telles que les téléphones portables, les radios, les équipements industriels ou les orages, ce qui peut entraîner des erreurs dans la transmission des données
- **Piratage du câble** : Les câbles peuvent être physiquement coupés ou endommagés pour interrompre la communication. **Rappel : Le wifi est un cable**
- **Écoute passive** : Les attaquants peuvent installer des dispositifs d'écoute passifs, tels que des capteurs acoustiques ou des fibres optiques, pour intercepter les signaux sans perturber la communication
- **Injection de signal** : Les attaquants peuvent injecter des signaux électromagnétiques ou optiques pour perturber la transmission des données

Pour minimiser les risques de sécurité de la couche 1 OSI, il est important d'adopter des mesures de sécurité physiques, telles que la protection des câbles, l'accès restreint aux installations de communication, la surveillance des signaux, la mise en place de systèmes d'alarme, etc.

La sécurité du réseau - Sécurité au niveau de la couche physique

Les attaques de la couche 1 sont des attaques physiques qui visent directement les composants matériels du réseau, tels que les câbles, les connecteurs, les amplificateurs, les répéteurs, etc.

Pour parer une attaque de la couche 1, voici quelques outils et logiciels utiles :

- **Testeur de câble** : Un testeur de câble est un outil qui permet de vérifier la continuité, les courts-circuits, les ouvertures et les croisements dans les câbles Ethernet. Il peut aider à détecter les câbles endommagés ou mal connectés, qui pourraient causer des problèmes de connectivité et de sécurité
- **Alimentation électrique ininterrompue (UPS)** : Une UPS est un dispositif qui fournit une alimentation de secours en cas de coupure de courant ou de fluctuations de tension. Elle peut protéger le matériel du réseau contre les coupures de courant et les pannes de l'alimentation électrique, qui pourraient causer des pertes de données ou des pannes du système
- **Gaine de protection des câbles** : Les gaines de protection des câbles sont des enveloppes qui protègent les câbles contre les dommages physiques, tels que les coupures, les perforations, les torsions ou les écrasements. Elles peuvent aider à protéger les câbles contre les attaques physiques, comme la coupure ou le sabotage
- **Système de vidéosurveillance** : Les systèmes de vidéosurveillance peuvent aider à surveiller et à détecter les activités suspectes autour des composants matériels du réseau, tels que les serveurs, les commutateurs, les routeurs, etc. Ils peuvent fournir des preuves vidéo utiles pour identifier les auteurs d'une attaque physique
- **Système de détection d'intrusion basé sur le comportement (BIDS)** : Les BIDS peuvent détecter les activités suspectes en surveillant les comportements du réseau et des utilisateurs. Ils peuvent identifier les anomalies dans les schémas de trafic ou les modèles d'utilisation qui pourraient indiquer une attaque de la couche 1

Il est important de noter que les outils et les logiciels ne peuvent pas garantir une protection complète contre les attaques de la couche 1, mais ils peuvent aider à détecter et à prévenir les attaques physiques avant qu'elles ne causent des dommages irréparables.

La sécurité du réseau - Sécurité au niveau de la couche liaison

La couche 2 du modèle OSI, également appelée couche liaison de données, est responsable de la transmission des données entre des nœuds adjacents sur le réseau. Cette couche est souvent vulnérable aux attaques de type "man-in-the-middle" où un attaquant intercepte et modifie les données en transit entre deux nœuds sur le réseau.

Voici quelques faiblesses de sécurité spécifiques de la couche 2 OSI :

- **Adressage MAC** : Les adresses MAC (Media Access Control) utilisées pour identifier les périphériques sur le réseau peuvent être falsifiées ou usurpées, ce qui peut permettre à un attaquant de se faire passer pour un périphérique autorisé sur le réseau.
- **ARP Spoofing** : Les attaquants peuvent envoyer de fausses réponses ARP (Address Resolution Protocol) pour associer leur adresse MAC à une adresse IP légitime, ce qui leur permet de recevoir le trafic destiné à cette adresse.
- **VLAN hopping** : Les attaquants peuvent utiliser des techniques de VLAN hopping pour accéder à des VLAN (Virtual Local Area Networks) qui ne leur sont pas autorisés.
- **Déni de service** : Les attaquants peuvent envoyer des trames de données volumineuses pour saturer la bande passante et perturber le trafic sur le réseau.
- **Frame Flooding Attacks** : Les attaquants peuvent envoyer des trames de données avec des adresses source falsifiées pour tromper les systèmes de sécurité et les pare-feu.

Pour minimiser les risques de sécurité de la couche 2 OSI, il est important d'adopter des mesures de sécurité telles que l'utilisation de VLAN pour isoler les segments de réseau, la configuration des commutateurs pour limiter l'accès au réseau, la surveillance des réponses ARP et la mise en place de systèmes de détection des attaques de déni de service.

La sécurité du réseau - Sécurité au niveau de la couche liaison

Les attaques de la couche 2 visent le protocole de liaison de données et les équipements de commutation, tels que les commutateurs et les ponts.

Pour parer une attaque de la couche 2, voici quelques outils et logiciels utiles :

- **Le protocole STP (Spanning Tree Protocol)** : Le protocole STP est conçu pour prévenir les boucles de commutation et les problèmes de connectivité qui pourraient causer des problèmes de sécurité. En activant STP, les commutateurs peuvent détecter les boucles et les désactiver en temps réel.
- **Le protocole DTP (Dynamic Trunking Protocol)** : Le protocole DTP est utilisé pour configurer automatiquement les ports d'un commutateur pour qu'ils fonctionnent en mode trunk ou access. Les administrateurs peuvent désactiver le DTP pour empêcher les attaquants de modifier la configuration du port et d'effectuer des attaques de type VLAN hopping.
- **Les listes de contrôle d'accès (ACL)** : Les ACL permettent de contrôler les accès aux réseaux et de limiter l'accès aux ports des commutateurs. Ils peuvent être utilisés pour bloquer les adresses MAC, les adresses IP et les protocoles spécifiques, et pour autoriser uniquement les connexions légitimes.
- **Les VLAN (Virtual Local Area Network)** : Les VLAN permettent de diviser un réseau en plusieurs segments logiques, ce qui permet d'isoler le trafic et de réduire le risque d'attaque. Les administrateurs peuvent configurer les VLAN pour que chaque segment soit traité comme un réseau distinct, ce qui peut renforcer la sécurité du réseau.
- **Les outils de détection d'intrusion (IDS)** : Les IDS sont des logiciels qui surveillent le trafic réseau et détectent les activités suspectes. Ils peuvent identifier les attaques de la couche 2, comme les attaques de type ARP poisoning ou MAC flooding, et signaler les événements suspects aux administrateurs.

Il est important de noter que ces outils et logiciels ne garantissent pas une protection complète contre les attaques de la couche 2, mais ils peuvent aider à prévenir et à détecter les attaques avant qu'elles ne causent des dommages importants. Les administrateurs doivent également prendre d'autres mesures de sécurité, comme la configuration appropriée des commutateurs, la mise à jour régulière des logiciels et l'utilisation de mots de passe forts.

La sécurité du réseau - Sécurité au niveau de la couche réseau

La couche 3 OSI, également appelée couche réseau, est responsable du routage des paquets de données entre les réseaux.

Voici quelques faiblesses de sécurité spécifiques à cette couche :

- **Attaques par déni de service (DoS)** : Les attaques DoS peuvent viser la couche 3 en inondant le réseau avec un grand nombre de paquets ou en envoyant des paquets malveillants qui sont destinés à épuiser les ressources du réseau
- **Attaques d'usurpation d'adresse IP** : Les attaquants peuvent modifier l'adresse IP source d'un paquet pour tromper les dispositifs de sécurité et les faire croire qu'il provient d'une source légitime, ce qui peut permettre aux attaquants de contourner les mécanismes de sécurité et d'effectuer des attaques malveillantes
- **Attaques de redirection de trafic** : Les attaques de redirection de trafic peuvent viser la couche 3 en modifiant les tables de routage pour rediriger le trafic vers des destinations malveillantes
- **Attaques de déni de service distribué (DDoS)** : Les attaques DDoS peuvent également viser la couche 3 en inondant le réseau avec un grand nombre de paquets provenant de plusieurs sources
- **Vulnérabilités du protocole de routage** : Les protocoles de routage utilisés par la couche 3 peuvent contenir des vulnérabilités qui permettent aux attaquants de manipuler le routage des paquets pour effectuer des attaques malveillantes

Pour minimiser ces faiblesses de sécurité, les administrateurs de réseau doivent mettre en place des mécanismes de sécurité, tels que les pare-feu, les routeurs sécurisés et les mécanismes de détection d'intrusion, pour détecter et prévenir les attaques malveillantes. De plus, il est important de mettre à jour régulièrement les logiciels et les dispositifs de sécurité pour assurer la sécurité du réseau.

La sécurité du réseau - Sécurité au niveau de la couche réseau

Les attaques de la couche 3 visent le protocole IP et les équipements de routage, tels que les routeurs.

Pour parer une attaque de la couche 3, voici quelques outils et logiciels utiles :

- **Les listes de contrôle d'accès (ACL)** : Les ACL peuvent être utilisées pour filtrer le trafic IP en fonction des adresses IP source et destination, des protocoles et des ports. Ils peuvent également être utilisés pour bloquer les adresses IP suspectes ou les attaques DDoS
- **Le protocole OSPF (Open Shortest Path First)** : OSPF est un protocole de routage dynamique qui utilise un algorithme pour calculer les chemins les plus courts entre les réseaux. Les administrateurs peuvent configurer OSPF pour bloquer les paquets qui ne sont pas autorisés à traverser le réseau, ce qui peut aider à prévenir les attaques
- **Les pare-feu** : Les pare-feu peuvent être utilisés pour filtrer le trafic entrant et sortant du réseau, et pour bloquer les attaques de type IP spoofing. Les pare-feu peuvent également être utilisés pour appliquer des politiques de sécurité, comme la limitation du trafic autorisé ou la surveillance du trafic suspect
- **Les VPN (Virtual Private Network)** : Les VPN sont utilisés pour sécuriser les communications entre les réseaux distants. Les VPN peuvent utiliser des protocoles de cryptage pour protéger les données sensibles et empêcher les attaques de type Man-in-the-Middle (MITM)
- **Les outils de détection d'intrusion (IDS)** : Les IDS peuvent être utilisés pour surveiller le trafic IP et détecter les activités suspectes, comme les scans de ports et les tentatives d'intrusion. Les IDS peuvent également être configurés pour bloquer les adresses IP ou les ports suspects

Il est important de noter que ces outils et logiciels ne garantissent pas une protection complète contre les attaques de la couche 3, mais ils peuvent aider à prévenir et à détecter les attaques avant qu'elles ne causent des dommages importants. Les administrateurs doivent également prendre d'autres mesures de sécurité, comme la configuration appropriée des routeurs, la mise à jour régulière des logiciels et l'utilisation de mots de passe forts.

SEC-LEC : Durcissement sécurité Linux

La sécurité du réseau - Daemons et serveurs

Les daemons et serveurs Linux sont deux concepts importants en matière d'administration système sur les systèmes d'exploitation Linux.

Un **daemon** est un programme informatique qui s'exécute en **arrière-plan sans intervention directe de l'utilisateur**. Les daemons sont souvent utilisés pour effectuer des tâches système, comme la gestion des imprimantes, la mise à jour de la base de données des utilisateurs, la surveillance des connexions réseau, etc. Les daemons peuvent être configurés pour se lancer automatiquement au démarrage du système, et pour s'exécuter en continu en arrière-plan.

Les **serveurs Linux**, quant à eux, sont des programmes informatiques qui **écoutent les connexions réseau et fournissent des services à d'autres ordinateurs connectés au réseau**. Les serveurs Linux sont souvent utilisés pour fournir des services tels que l'hébergement de sites web, la messagerie électronique, le partage de fichiers, la gestion de bases de données, etc. Les serveurs Linux peuvent fonctionner comme des daemons, c'est-à-dire qu'ils peuvent s'exécuter en arrière-plan, mais ils doivent écouter les connexions réseau pour répondre aux demandes des clients.

Il existe de nombreux daemons et serveurs Linux populaires, tels que le daemon de messagerie électronique Postfix, le serveur web Apache, le serveur de bases de données MySQL, le daemon de transfert de fichiers FTP, le daemon de contrôle de version Git, etc. Ces outils sont souvent utilisés par les administrateurs système pour fournir des services à d'autres utilisateurs ou pour automatiser des tâches système.

Les daemons et serveurs Linux peuvent être configurés et gérés à l'aide de la ligne de commande ou d'outils graphiques tels que Webmin. Les administrateurs système doivent s'assurer que les daemons et les serveurs Linux sont configurés de manière sécurisée et à jour pour éviter les vulnérabilités de sécurité.

SEC-LEC : Durcissement sécurité Linux

La sécurité du réseau - VPN

Un Virtual Private Network (VPN) est un réseau privé virtuel qui permet à des ordinateurs et des réseaux distants de communiquer de manière sécurisée en utilisant une connexion Internet publique. Les VPN sont de plus en plus utilisés pour accéder à des réseaux d'entreprise à distance, pour sécuriser les communications entre des sites distants, ou encore pour contourner la censure sur Internet.

Il existe deux principaux types de VPN : les VPN de niveau réseau (ou de niveau 3) et les VPN de niveau liaison (ou de niveau 2). Les VPN de niveau réseau utilisent le protocole IP pour acheminer le trafic entre les ordinateurs et les réseaux distants, tandis que les VPN de niveau liaison utilisent le protocole Ethernet pour connecter les ordinateurs et les réseaux distants.

- **Les VPN de niveau réseau** sont les plus courants. Ils utilisent généralement des protocoles de tunnelisation tels que IPSec (Internet Protocol Security), SSL (Secure Sockets Layer), ou encore OpenVPN pour encapsuler les données dans des paquets chiffrés et les transmettre en toute sécurité entre les ordinateurs et les réseaux distants. Les VPN de niveau réseau peuvent être configurés pour travailler avec la couche 3 (réseau) du modèle OSI, et sont souvent utilisés pour connecter des réseaux distants à travers des connexions Internet non sécurisées
- **Les VPN de niveau liaison** sont moins courants, mais sont parfois utilisés pour connecter des réseaux distants en utilisant des protocoles tels que L2TP (Layer 2 Tunneling Protocol), PPTP (Point-to-Point Tunneling Protocol), ou encore MPLS (Multiprotocol Label Switching). Les VPN de niveau liaison sont conçus pour travailler avec la couche 2 (liaison) du modèle OSI, et sont souvent utilisés pour connecter des ordinateurs distants ou pour étendre un réseau local (LAN) sur un réseau étendu (WAN)

En résumé, les VPN sont des outils puissants pour sécuriser les communications sur Internet et permettre la connectivité à distance. Les VPN de niveau réseau sont les plus courants et peuvent être configurés pour travailler avec la couche 3 du modèle OSI, tandis que les VPN de niveau liaison sont moins courants et sont conçus pour travailler avec la couche 2 du modèle OSI. Le choix du type de VPN dépend des besoins spécifiques de chaque utilisateur ou entreprise.

SEC-LEC : Durcissement sécurité Linux

La sécurité du réseau - VPN

Il existe différents types de connexions VPN en fonction des besoins spécifiques des utilisateurs ou des entreprises.

Parmi ces types, on trouve les connexions VPN site-à-site, les connexions VPN client-à-site, et les connexions VPN point-à-point :

- **Les connexions VPN site-à-site**, également appelées VPN LAN-to-LAN, permettent à deux réseaux locaux (LAN) distants de communiquer entre eux en utilisant une connexion VPN sécurisée. Les connexions VPN site-à-site sont souvent utilisées pour connecter des succursales d'entreprise ou des bureaux distants, pour permettre le partage de ressources, de fichiers et de données entre les réseaux locaux distants. Les connexions VPN site-à-site peuvent être configurées pour travailler avec la couche 3 (réseau) du modèle OSI, en utilisant des protocoles tels que IPSec, SSL ou OpenVPN
- **Les connexions VPN client-à-site**, également appelées VPN remote access, permettent aux utilisateurs distants de se connecter à un réseau local (LAN) en utilisant une connexion VPN sécurisée. Les connexions VPN client-à-site sont souvent utilisées pour permettre aux employés distants de se connecter au réseau de leur entreprise, pour accéder à des fichiers et des données, ou pour travailler à distance. Les connexions VPN client-à-site peuvent être configurées pour travailler avec la couche 3 (réseau) du modèle OSI, en utilisant des protocoles tels que IPSec, SSL ou OpenVPN
- **Les connexions VPN point-à-point** permettent à deux ordinateurs distants de communiquer directement entre eux en utilisant une connexion VPN sécurisée. Les connexions VPN point-à-point sont souvent utilisées pour permettre le partage de fichiers et de données entre deux ordinateurs distants, ou pour établir une connexion sécurisée entre deux réseaux locaux (LAN) distants. Les connexions VPN point-à-point peuvent être configurées pour travailler avec la couche 2 (liaison) du modèle OSI, en utilisant des protocoles tels que L2TP, PPTP ou MPLS

En résumé, les connexions VPN offrent une méthode sécurisée pour connecter des réseaux locaux (LAN) distants, des utilisateurs distants, ou des ordinateurs distants. Les connexions VPN site-à-site, client-à-site et point-à-point sont toutes des options populaires pour répondre aux besoins spécifiques des utilisateurs et des entreprises.

La sécurité du réseau - VPN

Voici un exemple de mise en place de WireGuard en point à point sous Ubuntu :

- Installer WireGuard sur les deux ordinateurs : *sudo apt install wireguard*
- Générer une clé privée et une clé publique sur les deux ordinateurs : *umask 077; wg genkey | tee privatekey | wg pubkey > publickey*
- Configurer le serveur (ordinateur 1) en créant un fichier de configuration */etc/wireguard/wg0.conf* avec le contenu suivant :

[Interface]
PrivateKey = <private key du serveur>
Address = 10.0.0.1/24

[Peer]
PublicKey = <public key du client>
AllowedIPs = 10.0.0.2/32

- Configurer le client (ordinateur 2) en créant un fichier de configuration */etc/wireguard/wg0.conf* avec le contenu suivant :

[Interface]
PrivateKey = <private key du client>
Address = 10.0.0.2/24

[Peer]
PublicKey = <public key du serveur>
AllowedIPs = 10.0.0.1/32
Endpoint = <adresse IP publique du serveur>:51820

SEC-LEC : Durcissement sécurité Linux

La sécurité du réseau - VPN

- Activer WireGuard sur les deux ordinateurs : *sudo wg-quick up wg0*
- Vérifier que la connexion est établie en exécutant la commande *sudo wg* sur les deux ordinateurs.
- La sortie devrait ressembler à ceci :

interface: wg0

public key: <public key de l'ordinateur>

private key: (hidden)

listening port: 51820

peer: <public key de l'autre ordinateur>

endpoint: <adresse IP publique de l'autre ordinateur>:51820

allowed ips: 10.0.0.1/32

latest handshake: <timestamp>

transfer: <nombre d'octets transférés>

Le port 51820 doit être ouvert sur le pare-feu du serveur pour permettre la communication avec le client. Les adresses IP et les clés privées/publiques doivent être remplacées par les valeurs réelles générées dans les étapes 2 et 3.

SEC-LEC : Durcissement sécurité Linux

La sécurité par la surveillance du système - L'utilitaire de consignation

Le système de consignation (ou journalisation) Linux est un mécanisme qui enregistre les événements système, tels que les messages du noyau, les erreurs des applications et les informations de débogage, dans des fichiers journaux pour un accès ultérieur.

Il existe deux utilitaires de consignation de base dans Linux :

- **syslog** est un démon qui collecte, enregistre et stocke des messages système dans des fichiers journaux. Les fichiers journaux sont stockés dans le répertoire /var/log. Les messages sont catégorisés par leur niveau de gravité, allant de "debug" à "emergency". Les messages peuvent également être acheminés vers des destinations externes, telles que des adresses email, des serveurs syslog distants, ou d'autres systèmes de consignation.
- **journald** est un système de consignation de journal plus récent qui est apparu avec la distribution Fedora en 2011, puis a été adopté par d'autres distributions Linux. Contrairement à syslog, journald stocke les fichiers journaux dans un format binaire plutôt que dans des fichiers texte. Les fichiers journaux sont stockés dans le répertoire /var/log/journal et peuvent être consultés à l'aide de la commande journalctl. journald offre également des fonctionnalités supplémentaires telles que la journalisation de méta-données supplémentaires telles que le temps d'exécution et le PID.

En général, journald est considéré comme étant plus efficace et plus rapide que syslog, en particulier pour les grands volumes de données. Cependant, syslog est toujours largement utilisé et prend en charge plus de destinations externes que journald.

Dans l'ensemble, l'utilitaire de consignation Linux est un outil important pour la surveillance, le dépannage et la résolution de problèmes système, et il est essentiel de savoir comment y accéder et l'utiliser pour les administrateurs système.

SEC-LEC : Durcissement sécurité Linux

La sécurité par la surveillance du système - L'utilitaire de consignation

La commande journalctl est l'utilitaire en ligne de commande pour accéder aux fichiers journaux générés par systemd-journald.

Voici quelques-unes des principales commandes journalctl pour un usage efficace :

- **journalctl** : Cette commande affiche les derniers messages du journal.
- **journalctl -u <unit>** : Cette commande affiche les messages liés à une unité spécifique. Par exemple, journalctl -u sshd affichera les messages liés au démon SSH.
- **journalctl -b** : Cette commande affiche les messages du journal depuis le début de la séance actuelle.
- **journalctl --list-boots** : Cette commande affiche une liste de tous les enregistrements de démarrage disponibles.
- **journalctl -k**: Cette commande affiche les messages du noyau.
- **journalctl --since <date>** : Cette commande affiche les messages du journal depuis une date spécifiée. Par exemple, journalctl --since "2022-02-01" affichera les messages du 1er février 2022.
- **journalctl --follow**: Cette commande affiche les messages en temps réel à mesure qu'ils sont générés.
- **journalctl -p <priority>** : Cette commande affiche les messages avec une priorité spécifiée. Les priorités vont de 0 (émergence) à 7 (débogage).
- **journalctl -o <format>** : Cette commande affiche les messages dans un format spécifié. Les formats disponibles incluent short, verbose, json, cat, export, json-pretty et json-sse.

Il est important de noter que journalctl offre de nombreuses autres options et filtres pour afficher et rechercher des messages spécifiques. L'utilisation de ces options peut grandement aider à diagnostiquer et à résoudre les problèmes système.

La sécurité par la surveillance du système - L'utilitaire de consignation

Les options **--user et --system** sont des commutateurs utiles pour journalctl, qui permettent de filtrer les messages du journal en fonction du contexte utilisateur ou système.

- **L'option --user** permet de filtrer les messages enregistrés par les processus appartenant à un utilisateur spécifique.

Par exemple, *journalctl --user* affiche les messages enregistrés par les processus de l'utilisateur actuel, tandis que *journalctl --user=username* affiche les messages enregistrés par les processus de l'utilisateur spécifié.

- **L'option --system** permet de filtrer les messages enregistrés par les processus système.

Par exemple, *journalctl --system* affiche les messages enregistrés par les processus du système, tels que systemd et les autres services système. Cette option est souvent utilisée pour filtrer les messages système à des fins de débogage.

Il est important de noter que l'option --system est utilisée par défaut si aucune option n'est spécifiée. Cela signifie que si vous exécutez simplement la commande journalctl, elle affichera les messages du système.

En résumé, l'option --user permet de filtrer les messages enregistrés par les processus appartenant à un utilisateur spécifique, tandis que l'option --system permet de filtrer les messages enregistrés par les processus système.

SEC-LEC : Durcissement sécurité Linux

La sécurité par la surveillance du système - Outils d'analyse des logs

Voici une brève description de quelques outils avancés d'analyse de logs Linux :

- AWStats : AWStats est un outil d'analyse de logs Web qui peut être utilisé pour générer des rapports détaillés sur les visiteurs de votre site Web. Il prend en charge la plupart des formats de fichiers journaux courants et peut également être utilisé pour détecter les attaques de piratage.
- Logcheck : Logcheck est un outil de surveillance de logs qui peut être utilisé pour détecter les anomalies dans les fichiers journaux système. Il est généralement utilisé pour surveiller les messages de log et les rapports de sécurité pour détecter les attaques potentielles.
- OSQuery : Osquery est un outil open source de surveillance de la sécurité des systèmes qui permet de collecter des données sur les systèmes d'exploitation en temps réel. Il peut être utilisé pour surveiller les activités suspectes et les comportements malveillants sur les serveurs et les ordinateurs de bureau.
- Wazuh (anciennement OSSEC) : Wazuh est un système open source de détection de logiciels malveillants, d'intégrité des fichiers et de surveillance de la sécurité. Il peut être utilisé pour surveiller les fichiers journaux système, les événements de sécurité et les alertes pour détecter les menaces potentielles.
- grafana : Grafana est une plate-forme open source de visualisation de données qui peut être utilisée pour afficher les données de log de manière graphique. Elle prend en charge de nombreux types de données et peut être utilisée pour créer des tableaux de bord de visualisation de logs en temps réel.
- Graylog : Graylog est une plate-forme open source de gestion de logs qui peut être utilisée pour collecter, agréger et analyser des logs de diverses sources. Elle est souvent utilisée dans les environnements de production pour surveiller et gérer les logs système à grande échelle.

Ces outils avancés peuvent être utilisés pour surveiller et analyser les fichiers journaux système de manière plus détaillée et efficace. Ils peuvent aider à détecter les menaces potentielles, les anomalies et les erreurs, et à fournir des rapports détaillés sur les activités système.

SEC-LEC : Durcissement sécurité Linux

La sécurité par la surveillance du système

Les sources de données comme Yara, SigmaHQ, SnortRules et autres sont des outils qui permettent de qualifier automatiquement les données des logs en utilisant des règles prédéfinies. Ces règles peuvent être utilisées pour détecter les modèles de comportement malveillant, les signatures de logiciels malveillants et les vulnérabilités connues.

- Yara est un outil open source de détection de logiciels malveillants qui permet de créer des règles de détection basées sur des chaînes de caractères, des expressions régulières et des conditions logiques. Il peut être utilisé pour détecter des logiciels malveillants connus ou inconnus en analysant les fichiers de log
- SigmaHQ est une collection de règles de détection de logiciels malveillants pour les outils SIEM. Les règles sont écrites en YAML et peuvent être facilement utilisées pour détecter les attaques de logiciels malveillants connus
- SnortRules est une collection de règles de détection de logiciels malveillants pour le système de prévention des intrusions Snort. Les règles sont écrites en langage propriétaire de Snort et peuvent être utilisées pour détecter les attaques de logiciels malveillants connus
- OpenCTI et MISP sont des outils de cyber-renseignement open source qui permettent de collecter et de partager des informations sur les menaces de sécurité. Ils peuvent être utilisés pour intégrer des sources de données de renseignement sur les menaces de sécurité avec des fichiers de logs pour améliorer la détection des menaces et des vulnérabilités

En utilisant ces sources de données, les équipes de sécurité peuvent améliorer la détection des menaces et réduire le temps nécessaire pour détecter et répondre aux incidents de sécurité.

La sécurité par la surveillance du système - Le dispositif d'accounting system

Un dispositif d'accounting est un système de suivi de l'utilisation des ressources d'un système informatique. Il permet de collecter des informations sur l'utilisation des ressources telles que le temps d'utilisation du processeur, la consommation de mémoire, les entrées/sorties sur le disque, les requêtes réseau, etc.

Le but d'un dispositif d'accounting est de suivre les ressources utilisées par les utilisateurs ou les processus, afin de pouvoir facturer ces ressources, ou d'optimiser leur utilisation en fonction des besoins.

En pratique, un dispositif d'accounting peut être implémenté de différentes manières, selon les besoins de l'utilisateur. Il peut s'agir d'un ensemble de scripts qui collectent les données d'utilisation des ressources à partir de différents outils du système, ou d'un outil intégré au système d'exploitation qui collecte automatiquement les données d'utilisation des ressources.

Parmi les outils d'accounting couramment utilisés sur les systèmes Linux, on peut citer :

- **systemd** : le système d'initialisation systemd inclut un outil d'accounting qui peut collecter des informations sur les ressources utilisées par les processus.
- **atop** : un outil d'accounting avancé pour Linux qui fournit des informations détaillées sur l'utilisation des ressources système.
- **auditd** : un outil de surveillance et de journalisation des événements du système qui peut être utilisé pour collecter des informations sur l'utilisation des ressources.
- **psacct** : un ensemble d'utilitaires qui collectent des informations sur l'utilisation des ressources système, y compris le temps d'utilisation du processeur et les entrées/sorties sur le disque.

Ces outils d'accounting peuvent être utilisés pour surveiller l'utilisation des ressources et générer des rapports sur les tendances d'utilisation des ressources, pour optimiser l'utilisation des ressources système. Ils peuvent également être utilisés pour facturer les clients en fonction de leur utilisation des ressources informatiques, dans le cadre d'un modèle de tarification basé sur l'utilisation.

SEC-LEC : Durcissement sécurité Linux

La sécurité par la surveillance du système - Le dispositif d'accounting system

auditd est un outil de surveillance et de journalisation des événements du système pour Linux. Il permet de suivre les événements importants du système et de générer des alertes en cas de comportements anormaux. auditd peut être utilisé pour surveiller les fichiers et répertoires système, les modifications des fichiers de configuration, l'activité réseau, l'utilisation des ressources système et bien plus encore.

Pour installer auditd sur un système Linux, il suffit d'utiliser la commande appropriée pour votre distribution.

Par exemple, vous pouvez utiliser la commande suivante : *sudo apt-get install auditd*

Une fois installé, auditd doit être configuré avec des règles pour spécifier les événements qui doivent être surveillés. Ces règles sont généralement stockées dans le fichier de configuration /etc/audit/audit.rules.

Voici un exemple simple de règle pour surveiller l'accès aux fichiers dans le répertoire /etc : *-w /etc -p wa -k etc-access*

Cette règle spécifie que toute opération d'écriture (w) ou d'accès (a) aux fichiers dans le répertoire /etc doit être surveillée, et un message de journalisation avec la clé etc-access doit être généré.

Voici quelques commandes utiles pour travailler avec auditd :

- **auditctl** : une commande pour ajouter, supprimer ou lister des règles pour auditd
- **ausearch** : une commande pour rechercher les journaux d'audit en fonction de différents critères, tels que la date, l'utilisateur ou le type d'événement
- **aureport** : une commande pour générer des rapports sur les événements d'audit, tels que les tentatives d'accès non autorisées ou les modifications de fichiers
- **auditd** : la commande pour démarrer, arrêter ou redémarrer le service auditd

Avec ces commandes, vous pouvez surveiller les activités du système et générer des alertes en cas d'activités suspectes ou non autorisées. Cependant, pour obtenir les avantages complets de l'outil, il est recommandé de mettre en place une configuration complète d'auditd avec des règles appropriées.

La sécurité par la surveillance du système - Le dispositif d'accounting system

Il est également possible d'utiliser des règles externes pour auditd, par exemple à partir de projets tels que CIS (Center for Internet Security) ou STIG (Security Technical Implementation Guide). Ces règles peuvent fournir des configurations de sécurité prêtes à l'emploi pour différents environnements, ou des règles pour répondre aux exigences de conformité spécifiques.

auditctl -l liste les règles actives

Les règles d'audit sont complexes. Des gens en propose des toutes faites :

- auditd-userspace : Des règles du développeur d'audits
- auditd-attack : Des règles en lien avec la fameuse taxonomie Mitre Att&ck
- auditd : Des règles généralistes issues des meilleures sources

À mettre dans /etc/audit/rules.d/.

Il n'est pas obligatoire de toutes les télécharger, ni de toutes les activer, au risque de ralentir le système. Seules les règles pertinentes pour votre contexte doivent être validées.

Des Questions

SEC-LEC : Durcissement sécurité Linux
Le patch management

SEC-LEC : Durcissement sécurité Linux

La sécurité par la surveillance du système - Mise à jour du système

La gestion des correctifs (ou patch management en anglais) sous Linux est un processus important pour maintenir la sécurité et la stabilité de votre système.

Voici quelques étapes que vous pouvez suivre pour gérer les correctifs sous Linux :

- **Utilisez un gestionnaire de paquets** : Les gestionnaires de paquets tels que pat, dnf ou Pacman vous permettent de gérer facilement les mises à jour du système. Ils vous permettent de mettre à jour tous les logiciels installés sur votre système en une seule commande
- **Configurez les sources de mises à jour** : Les sources de mises à jour définissent les serveurs à partir desquels votre système téléchargera les mises à jour. Assurez-vous de configurer les sources de mises à jour pour votre distribution Linux pour vous assurer que vous recevez les derniers correctifs
- **Planifiez les mises à jour régulières** : Mettez en place une planification régulière pour les mises à jour de votre système, par exemple une fois par semaine. Cela vous permettra de maintenir votre système à jour et d'appliquer les correctifs de sécurité dès leur publication
- **Surveillez les notifications de sécurité** : Les fournisseurs de distribution Linux publient régulièrement des notifications de sécurité pour les vulnérabilités connues. Soyez à l'écoute de ces notifications et appliquez rapidement les correctifs de sécurité recommandés
- **Testez les mises à jour avant de les déployer en production** : Il est important de tester les mises à jour avant de les déployer en production pour éviter les erreurs et les problèmes de compatibilité

En suivant ces étapes, vous pouvez gérer efficacement les correctifs sous Linux et maintenir la sécurité et la stabilité de votre système.

La sécurité par la surveillance du système - Mise à jour du système

Il existe plusieurs outils disponibles pour le déploiement en masse de nouvelles versions de packages sous Linux.

Voici quelques-uns des outils les plus couramment utilisés :

- Ansible : Ansible est un outil de gestion de configuration open source qui peut être utilisé pour le déploiement de packages en masse. Il utilise un langage simple et intuitif appelé YAML pour décrire les tâches à effectuer et peut être utilisé pour gérer des systèmes distribués de toutes tailles.
- Puppet : Puppet est un autre outil de gestion de configuration open source qui peut être utilisé pour le déploiement de packages en masse. Il utilise un langage de configuration spécifique appelé Puppet DSL ou directement ruby pour décrire les états souhaités des systèmes et peut être utilisé pour automatiser la configuration, la gestion et le déploiement des logiciels.
- SaltStack : SaltStack est une plateforme de gestion d'infrastructure open source qui peut être utilisée pour le déploiement en masse de nouvelles versions de packages. Elle utilise un langage de configuration appelé SaltState pour décrire les états souhaités des systèmes et peut être utilisée pour la gestion de systèmes distribués et de grande envergure.

Ces outils offrent une solution pratique pour le déploiement en masse de nouvelles versions de packages sous Linux. Il est important de choisir l'outil le mieux adapté à votre environnement spécifique et à vos besoins de déploiement.

Des Questions

SEC-LEC : Durcissement sécurité Linux
Les sondes de détection d'intrusions

Les sondes de détection d'intrusions - Les Intrusion Detection System (IDS)

Un IDS (Intrusion Detection System) est un système de sécurité informatique conçu pour surveiller et analyser les événements sur un réseau ou un système informatique, afin de détecter toute tentative d'intrusion ou d'attaque malveillante. L'objectif principal d'un IDS est de détecter les activités suspectes, de signaler les violations de sécurité et d'alerter les administrateurs du système afin qu'ils puissent prendre les mesures nécessaires pour contrer les menaces.

Les IDS peuvent être gérés soit par des règles prédéfinies, soit par des techniques d'IA.

- **Les IDS gérés par des règles prédéfinies** sont conçus pour détecter les activités suspectes en comparant les événements observés sur le réseau avec un ensemble de règles prédéfinies. Ces règles sont basées sur des schémas d'attaques connus ou des comportements considérés comme anormaux. Les IDS basés sur des règles sont relativement simples à déployer et à gérer, mais ils ont tendance à générer un grand nombre de faux positifs, c'est-à-dire des alertes qui ne sont pas liées à des activités malveillantes réelles.
- **Les IDS basés sur l'IA** sont conçus pour surmonter les limites des IDS basés sur des règles en utilisant des techniques d'apprentissage automatique pour analyser les événements réseau et identifier les comportements anormaux. Ces IDS sont capables de s'adapter aux nouvelles menaces et de découvrir de nouveaux modèles de trafic sans intervention humaine. Les IDS basés sur l'IA sont plus efficaces pour détecter les attaques sophistiquées et les activités malveillantes non détectées par les IDS basés sur des règles. Cependant, leur mise en œuvre et leur gestion peuvent être plus complexes en raison de la nécessité de former les algorithmes d'IA et de les maintenir à jour.

Dans tous les cas, il est important de noter que les IDS ne peuvent pas offrir une protection à 100 % contre toutes les menaces de sécurité. Les IDS sont un outil de sécurité supplémentaire qui peut aider à réduire les risques de sécurité et à minimiser les dommages en cas d'attaque réussie. Les IDS doivent être utilisés en conjonction avec d'autres mesures de sécurité telles que les pare-feux, les systèmes de prévention des intrusions et les pratiques de sécurité informatique de base pour offrir une protection complète contre les menaces de sécurité.

Les sondes de détection d'intrusions - Les Intrusion Prevention System (IPS)

Un IPS (Intrusion Prevention System) est un système de sécurité informatique qui agit comme une extension de l'IDS (Intrusion Detection System) en ajoutant une couche de prévention. Alors que l'IDS est conçu pour détecter les menaces de sécurité en surveillant les événements sur un réseau ou un système informatique, l'IPS est conçu pour prendre des mesures immédiates pour bloquer les attaques en temps réel.

Un IPS utilise plusieurs méthodes pour bloquer le trafic malveillant détecté par l'IDS :

- **Bloquer le trafic en fonction de règles prédéfinies** : L'IPS peut être configuré pour bloquer le trafic en fonction de règles prédéfinies. Ces règles peuvent être basées sur des signatures d'attaques connues, des adresses IP, des ports ou des protocoles spécifiques. Si le trafic correspond à l'une de ces règles, l'IPS peut le bloquer immédiatement.
- **Utiliser des analyses comportementales pour bloquer le trafic** : L'IPS peut utiliser des analyses comportementales pour détecter les activités malveillantes qui ne sont pas détectées par des règles prédéfinies. Par exemple, si un utilisateur tente de se connecter à plusieurs serveurs en même temps ou si un serveur essaie de se connecter à un grand nombre d'adresses IP différentes en peu de temps, l'IPS peut considérer cela comme une activité suspecte et bloquer le trafic.
- **Bloquer le trafic en utilisant l'apprentissage automatique** : L'IPS peut également utiliser l'apprentissage automatique pour détecter les menaces de sécurité. L'IPS analyse les données de trafic pour identifier les modèles d'activité qui sont associés à des attaques. Une fois que l'IPS a identifié ces modèles, il peut bloquer le trafic correspondant.
- **Utiliser des technologies de virtualisation** : L'IPS peut utiliser des technologies de virtualisation pour isoler les systèmes infectés et empêcher la propagation de l'infection. Par exemple, l'IPS peut créer une machine virtuelle pour un système infecté et isoler cette machine virtuelle du reste du réseau.

En résumé, l'IPS utilise une variété de méthodes pour bloquer le trafic malveillant détecté par l'IDS, y compris l'utilisation de règles prédéfinies, d'analyses comportementales, d'apprentissage automatique et de technologies de virtualisation.

SEC-LEC : Durcissement sécurité Linux

Les sondes de détection d'intrusions - Les Netword-based Intrusion Detection System (NIDS)

Un NIDS (Network Intrusion Detection System) est un système de détection d'intrusion réseau qui surveille le trafic réseau pour détecter les activités malveillantes. Contrairement à l'IPS (Intrusion Prevention System), qui bloque le trafic malveillant en temps réel, le NIDS se contente de détecter les activités suspectes et de les signaler à un administrateur système ou à une console de gestion.

Le NIDS peut être déployé sur un réseau pour surveiller le trafic entrant et sortant. Il analyse les paquets de données à la recherche de signatures ou de modèles d'activité suspecte. Le NIDS peut être configuré pour détecter les attaques en se basant sur des signatures connues, ou en utilisant des techniques d'analyse comportementale pour détecter les activités malveillantes qui ne correspondent pas à des signatures connues.

Le NIDS peut être utilisé pour détecter une variété d'activités malveillantes, telles que des scans de port, des tentatives d'authentification non autorisées, des attaques par déni de service, des tentatives de détournement de session, des tentatives d'injection SQL, entre autres. Lorsqu'une activité suspecte est détectée, le NIDS génère une alerte qui peut être envoyée à un administrateur système ou à une console de gestion pour enquête et traitement.

En somme, le NIDS est un outil important pour la surveillance de la sécurité des réseaux informatiques. Il permet de détecter rapidement les activités malveillantes et d'alerter les administrateurs système pour prendre des mesures appropriées.

Les sondes de détection d'intrusions - Les Netword-based Intrusion Detection System (NIDS)

Voici quelques exemples de NIDS open source :

- Snort : C'est l'un des outils NIDS open source les plus populaires et les plus utilisés. Il utilise des règles pour détecter les attaques et les intrusions sur le réseau
- Suricata : Un autre NIDS open source, Suricata est conçu pour être hautement évolutif et capable de gérer des charges de travail à grande échelle
- Zeek (anciennement appelé "Bro") : Zeek est un NIDS open source basé sur le langage de script "Bro Script". Il est conçu pour être facilement extensible et personnalisable
- Wazuh (anciennement OSSEC): En plus de la détection d'intrusion réseau, OSSEC est également un HIDS open source qui surveille l'activité système sur un hôte local
- Security Onion : Il s'agit d'une distribution de Linux open source qui intègre plusieurs outils de sécurité, y compris Snort, Suricata et Bro, pour fournir une plateforme complète de détection d'intrusion

Ces outils NIDS open source offrent des fonctionnalités similaires à celles des solutions commerciales, mais ils peuvent nécessiter davantage de connaissances techniques pour la configuration et la maintenance. Cependant, ils peuvent être une alternative économique et efficace pour les organisations disposant de ressources limitées pour la sécurité informatique.

Les sondes de détection d'intrusions - Les Network-based Intrusion Detection System (NIDS)

Pour déployer la version Docker de SELKS, vous pouvez suivre les étapes suivantes :

- Assurez-vous que Docker est installé sur votre système. Vous pouvez installer Docker en suivant les instructions de la documentation officielle : https://docs.docker.com/get-docker/
- Réalisez les actions suivantes :

```
git clone https://github.com/StamusNetworks/SELKS.git
cd SELKS/docker/
./easy-setup.sh
docker-compose up -d
```

- Une fois que les containers ont fini de démarrer, il vous suffit de pointer votre browser vers https://your.selks.IP.here/
- Si vous avez, pendant l'installation, choisi Portainer, vous devez configurer ses logins et mot de passe à https://your.selks.IP.here:9443
- Vous devriez voir l'interface utilisateur de SELKS, où vous pouvez configurer les règles de détection, afficher les journaux d'événements, etc.

Voilà, votre instance SELKS est maintenant opérationnelle et prête à être utilisée pour la détection d'intrusion sur votre système.

Les sondes de détection d'intrusions - Les Netword-based Intrusion Prevention System (NIPS)

Le **NIPS (Network Intrusion Prevention System)** est un système de sécurité informatique qui surveille le trafic réseau pour détecter et prévenir les activités malveillantes. Contrairement au NIDS (Network Intrusion Detection System) qui ne fait que détecter les intrusions, le NIPS est conçu pour bloquer les tentatives d'intrusion en temps réel.

Le NIPS utilise des techniques similaires à celles de l'IDS et de l'IPS, mais en combinant la surveillance en temps réel avec la capacité de bloquer le trafic malveillant. Il peut être déployé sur un réseau pour surveiller le trafic entrant et sortant et analyser les paquets de données à la recherche de signatures ou de modèles d'activité suspecte.

Lorsqu'une activité malveillante est détectée, le NIPS peut prendre des mesures immédiates pour la bloquer, comme bloquer l'adresse IP de l'attaquant, fermer les ports, arrêter la communication avec un serveur malveillant, ou encore limiter le débit du trafic.

Le NIPS est particulièrement utile dans les environnements à haute disponibilité où le temps de réponse est critique. Il permet de réduire le temps nécessaire pour identifier et bloquer les attaques potentielles, en automatisant le processus de blocage des attaques. Cela réduit également la charge de travail des administrateurs système et améliore la sécurité globale du réseau.

En somme, le NIPS est un système de sécurité avancé qui permet de protéger les réseaux informatiques contre les menaces potentielles en détectant et bloquant les activités malveillantes en temps réel.

Les sondes de détection d'intrusions - Les Host-based Intrusion Detection System (HIDS)

Un HIDS (Host-based Intrusion Detection System) est un système de détection d'intrusion qui surveille les activités sur un ordinateur individuel ou un système d'exploitation. Contrairement à un NIDS (Network Intrusion Detection System), qui surveille le trafic réseau, le HIDS est conçu pour surveiller les activités sur l'hôte local et détecter les activités malveillantes telles que l'installation de logiciels malveillants, la modification de fichiers système, les tentatives d'attaques de type brute force, etc.

Le HIDS est généralement déployé sur des systèmes individuels pour surveiller les fichiers système, les journaux d'événements, les processus en cours d'exécution et d'autres activités qui pourraient indiquer une intrusion. Il peut être configuré pour détecter les activités malveillantes en utilisant des signatures connues ou en utilisant des techniques d'analyse comportementale pour identifier les activités qui ne correspondent pas à des modèles connus.

Lorsqu'une activité suspecte est détectée, le HIDS peut générer une alerte, envoyer un e-mail ou exécuter une commande pour bloquer l'activité malveillante. Le HIDS peut également stocker les journaux d'activité pour une analyse ultérieure.

Le HIDS est un outil important pour la surveillance de la sécurité des systèmes d'exploitation et des ordinateurs individuels. Il permet de détecter rapidement les activités malveillantes et d'alerter les administrateurs système pour prendre des mesures appropriées pour limiter les dommages. Cependant, il convient de noter que le HIDS a des limites, car il ne peut pas détecter les activités malveillantes qui se produisent en dehors de l'hôte local, ce qui nécessite l'utilisation d'un NIDS pour surveiller le trafic réseau.

SEC-LEC : Durcissement sécurité Linux

Les sondes de détection d'intrusions

Voici quelques exemples de HIDS (Host Intrusion Detection System) open source :

- **OSSEC**: OSSEC est l'un des HIDS open source les plus populaires. Il utilise des règles préétablies pour détecter les intrusions sur un système hôte et peut également surveiller les fichiers, les journaux système et les bases de données
- **Tripwire**: Tripwire est un HIDS open source qui est utilisé pour surveiller les fichiers et les répertoires sur un système hôte. Il peut détecter les modifications apportées aux fichiers, ce qui peut indiquer une compromission du système
- **AIDE**: AIDE (Advanced Intrusion Detection Environment) est un autre HIDS open source qui surveille les fichiers, les répertoires et les journaux système pour détecter les intrusions. Il utilise des règles préétablies pour détecter les changements dans le système
- **Samhain**: Samhain est un HIDS open source qui peut être utilisé pour surveiller les fichiers, les répertoires et les processus sur un système hôte. Il utilise des règles préétablies pour détecter les intrusions et peut également envoyer des alertes par e-mail
- **Rookit Hunter**: Rootkit Hunter est un HIDS open source qui est utilisé pour détecter les rootkits et les autres types de logiciels malveillants sur un système hôte. Il effectue des vérifications de l'intégrité des fichiers et des processus pour détecter les modifications non autorisées

Ces exemples ne sont pas exhaustifs et il existe de nombreux autres HIDS open source disponibles sur le marché.

SEC-LEC : Durcissement sécurité Linux

Les sondes de détection d'intrusions

Fail2ban, DenyHosts et SSHGuard sont des exemples de HIDS (Host Intrusion Detection System) open source qui se concentrent sur la détection et la prévention des attaques sur des serveurs.

- **Fail2ban** : Fail2ban est un HIDS open source qui surveille les journaux de serveurs tels que SSH, Apache et Nginx, et détecte les attaques répétitives. Lorsqu'une attaque est détectée, Fail2ban bloque l'adresse IP de l'attaquant à l'aide d'un pare-feu
- **DenyHosts** : DenyHosts est un HIDS open source spécialement conçu pour protéger les serveurs SSH. Il surveille les journaux d'authentification SSH et détecte les tentatives de connexion échouées répétitives. DenyHosts bloque automatiquement l'adresse IP de l'attaquant à l'aide d'un pare-feu
- **SSHGuard** : SSHGuard est un autre HIDS open source qui surveille les journaux d'authentification SSH et bloque automatiquement les adresses IP des attaquants en utilisant un pare-feu. SSHGuard peut également détecter et bloquer les attaques sur d'autres services réseau tels que FTP, SMTP et POP3

Ces outils sont particulièrement utiles pour protéger les serveurs contre les attaques de force brute, qui sont des tentatives répétées pour deviner les mots de passe en essayant de nombreuses combinaisons de mots de passe. En bloquant les adresses IP des attaquants, ces outils peuvent aider à réduire le nombre de tentatives d'authentification échouées et à améliorer la sécurité des serveurs.

SEC-LEC : Durcissement sécurité Linux

Les sondes de détection d'intrusions - Les Host-based Intrusion Prevention System (HIPS)

Un HIPS (Host-based Intrusion Prevention System) est un système de sécurité informatique qui fonctionne sur l'hôte local pour prévenir les intrusions en bloquant les activités malveillantes avant qu'elles ne puissent causer des dommages. Il utilise des mécanismes de détection similaires à ceux d'un HIDS pour surveiller les activités sur l'hôte local, mais il prend également des mesures proactives pour empêcher les intrusions.

Un HIPS peut être configuré pour bloquer les activités malveillantes en utilisant des techniques telles que la mise en liste noire ou blanche, la restriction des accès, l'application de politiques de sécurité, etc. Il peut également être intégré avec d'autres outils de sécurité pour fournir une défense en profondeur.

Le HIPS est particulièrement utile dans les environnements où des applications critiques sont en cours d'exécution, telles que les systèmes de contrôle industriel ou les systèmes d'information des entreprises. En bloquant les activités malveillantes avant qu'elles ne puissent causer des dommages, le HIPS peut aider à maintenir la disponibilité des systèmes et à garantir la confidentialité et l'intégrité des données.

Cependant, le HIPS peut être difficile à configurer et à gérer en raison de son impact sur les performances et de sa sensibilité aux faux positifs. Il est donc important de bien comprendre les besoins de sécurité de l'organisation et de mettre en place une politique de sécurité claire pour garantir que le HIPS est configuré de manière optimale.

Les sondes de détection d'intrusions - Modèle de déploiement

Les gros IDS/IPS (Intrusion Detection/Prevention Systems) sont souvent déployés en utilisant un modèle de déploiement classique appelé modèle en boîte à outils.

Ce modèle consiste à déployer un certain nombre de sondes de surveillance sur différents segments de réseau pour collecter et agréger les données d'activité réseau. Ces sondes sont ensuite reliées à un ou plusieurs systèmes de gestion de l'IDS/IPS qui effectuent l'analyse et la corrélation des événements, ainsi que la prise de décision pour la prévention des intrusions.

Le modèle en boîte à outils est souvent utilisé dans les grandes entreprises, les fournisseurs de services et les organisations gouvernementales qui ont des réseaux étendus et des exigences de sécurité élevées. Les IDS/IPS sont déployés dans des emplacements stratégiques sur le réseau, tels que les points d'entrée, les points de sortie, les points de passage obligatoire et les segments critiques. Ils sont souvent installés dans des boîtiers matériels dédiés, des serveurs virtuels ou des appliances de sécurité, qui sont équipés de processeurs rapides et de grandes quantités de mémoire pour pouvoir gérer la charge de trafic.

Le modèle en boîte à outils permet aux IDS/IPS de surveiller et de prévenir les intrusions dans les environnements réseau distribués, ce qui est essentiel pour les organisations qui doivent protéger leurs réseaux contre les menaces de sécurité. Cependant, ce modèle peut être coûteux en raison des coûts initiaux d'achat et de déploiement des sondes et des systèmes de gestion de l'IDS/IPS, ainsi que des coûts continus de maintenance et de gestion des systèmes.

OSSEC et Tripwire

La présentation de OSSEC et son remplacement par Wazuh a déjà été faite.

Tripwire, quand à lui, est devenu propriétaire.

Le code source sur github OST n'a pas évolué depuis au moins 2018.

La dernière release 2.4.3.7 date du 31 mars 2018.
La prochaine release 2.4.3.8 est dans les pull request depuis le 16 mars 2019.

Les sondes de détection d'intrusions - OSSIM

Un **SIEM (Security Information and Event Management)** est un outil de sécurité informatique conçu pour collecter, analyser et corréler les données de sécurité provenant de diverses sources dans un environnement informatique.

Les données de sécurité collectées peuvent inclure des journaux d'événements système, des informations de flux de réseau, des alertes de sécurité, des informations sur les vulnérabilités et d'autres types de données de sécurité.

Le SIEM analyse ces données à l'aide d'algorithmes et de techniques d'apprentissage automatique pour détecter des anomalies, des comportements malveillants et des attaques potentielles.

Le SIEM peut également fournir des fonctions de surveillance en temps réel, d'alerte et de reporting pour aider les équipes de sécurité à détecter et à répondre rapidement aux menaces de sécurité.

En somme, le SIEM est un outil essentiel pour les entreprises souhaitant renforcer leur posture de sécurité informatique en permettant une visibilité complète de leur environnement, la détection précoce des menaces potentielles et la réponse rapide aux incidents de sécurité.

OSSIM a été racheté par AT@T et a disparu.

SEC-LEC : Durcissement sécurité Linux

Les sondes de détection d'intrusions - File Integrity Management (FIM)

Un FIM (File Integrity Manager) est un logiciel conçu pour surveiller l'intégrité des fichiers sur un système informatique.

Il utilise des algorithmes de hachage pour vérifier si les fichiers ont été modifiés de manière inattendue, altérés ou supprimés, en comparant les empreintes des fichiers enregistrées dans une base de données de référence avec celles des fichiers actuels.

Si une différence est détectée, le FIM génère une alerte pour informer l'administrateur du système ou un opérateur de sécurité de l'incident et leur permet de prendre les mesures nécessaires pour remédier à la situation.

Le FIM est souvent utilisé dans les environnements de conformité réglementaire et de sécurité informatique, où il est important de maintenir l'intégrité des données et de détecter rapidement toute activité suspecte.

Il existe plusieurs FIM open source disponibles, chacun avec ses propres fonctionnalités et avantages. Voici une description de certains des principaux FIM open source :

- AIDE - Advanced Intrusion Detection Environment : AIDE est un FIM open source qui peut surveiller les fichiers et les répertoires pour détecter les modifications apportées par un intrus ou un programme malveillant. Il peut également être utilisé pour surveiller les journaux système et les paramètres de configuration pour détecter les changements non autorisés
- SAMHAIN/BELTANE : Samhain est un FIM open source qui peut surveiller les fichiers, les répertoires, les journaux système et les paramètres de configuration pour détecter les modifications non autorisées. Il peut également être utilisé pour surveiller les connexions réseau et les processus en cours d'exécution pour détecter les activités suspectes
- Wazuh : Wazuh est un système de détection d'intrusion open source qui peut être utilisé comme FIM pour surveiller les fichiers, les répertoires, les registres de système, les journaux et d'autres éléments de configuration. Il utilise des techniques d'analyse de log pour détecter les comportements suspects et envoie des alertes en temps réel en cas de violation. Wazuh dispose également d'une interface graphique utilisateur (GUI) pour une gestion facile et une visualisation des alertes
- Afick est un FIM open source pour les systèmes Unix et Linux. Il utilise des algorithmes de hachage pour surveiller les fichiers et les répertoires pour détecter les modifications non autorisées. Afick peut être configuré pour surveiller différents aspects du système, y compris les fichiers, les permissions, les propriétaires, les dates de modification, les liens symboliques et les processus en cours d'exécution.Afick stocke les informations de surveillance dans une base de données pour une vérification ultérieure et dispose d'un mode interactif pour la vérification des différences de fichiers. Il peut également envoyer des alertes par e-mail en cas de modifications non autorisées et dispose d'un support multi-langue pour une utilisation dans différents pays. Afick est assez simple à installer et à utiliser, mais peut nécessiter une configuration initiale pour s'assurer qu'il surveille les fichiers et les répertoires pertinents. Il est particulièrement adapté pour les petits et moyens environnements, et peut être utilisé pour renforcer la sécurité dans les systèmes d'information critiques

Les sondes de détection d'intrusions - FIM (File Integrity Management)

linpeas est un outil open-source d'escalade de privilèges pour les systèmes Linux. Il se concentre sur la recherche de vulnérabilités et d'exploits qui pourraient être utilisés pour obtenir des privilèges élevés sur un système Linux.

LinPEAS est conçu pour être utilisé par les professionnels de la sécurité et les administrateurs système pour auditer la sécurité de leurs systèmes Linux. Il utilise des scripts shell pour effectuer des tâches telles que la recherche de fichiers SUID, la vérification des autorisations de fichiers et de répertoires, la recherche de services et de fichiers de configuration, et la recherche d'autres signes de vulnérabilités.

LinPEAS est hautement personnalisable, ce qui permet aux utilisateurs de spécifier les vérifications à effectuer et d'exclure des éléments de la vérification s'ils ne sont pas pertinents. Il est également régulièrement mis à jour pour inclure des nouvelles fonctionnalités et des corrections de bugs.

Cependant, comme pour tout outil de sécurité, il est important d'utiliser LinPEAS avec prudence et de vérifier les résultats avec soin avant de prendre des mesures pour remédier aux vulnérabilités détectées.

SEC-LEC : Durcissement sécurité Linux

Les sondes de détection d'intrusions - FIM (File Integrity Management)

Voici les étapes pour installer et utiliser LinPEAS sur un système Linux :

- Télécharger le script LinPEAS depuis le référentiel Github officiel : linpeas
  wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh
- Donner des autorisations d'exécution au script en utilisant la commande suivante : *chmod +x linpeas.sh*
- Exécuter le script en tant que super-utilisateur : *sudo ./linpeas.sh*

Attendez que le script soit exécuté et qu'il affiche les résultats. Les résultats seront affichés dans le terminal.

- Vous pouvez également rediriger les résultats vers un fichier en utilisant la commande suivante :
  sudo ./linpeas.sh > resultat.txt

LinPEAS effectuera une analyse du système pour détecter les vulnérabilités et les faiblesses potentielles qui pourraient être exploitées pour l'escalade des privilèges. Le script affichera les résultats dans le terminal et les enregistrera également dans un fichier texte.

Il est important de noter que les résultats de LinPEAS doivent être interprétés avec soin et vérifiés par des professionnels de la sécurité qualifiés avant de prendre toute mesure pour remédier aux vulnérabilités détectées.

Des Questions

SEC-LEC : Durcissement sécurité Linux
Durcissement complémentaire

SEC-LEC : Durcissement sécurité Linux

Durcissement complémentaire - Durcissement des serveurs Web

Le durcissement d'un reverse proxy web est important pour améliorer la sécurité du système.

Voici quelques étapes qui peuvent être suivies pour durcir un reverse proxy web :

- **Configuration du pare-feu** : Configurez le pare-feu pour autoriser uniquement les connexions entrantes et sortantes nécessaires. Vous pouvez bloquer l'accès à tous les ports, sauf ceux qui sont nécessaires pour le reverse proxy.
- **Configurer le SSL/TLS** : Utilisez SSL/TLS pour chiffrer la communication entre le client et le reverse proxy. Il est important de configurer des certificats SSL/TLS valides pour le domaine du site web.
- **Configuration du chiffrement** : Utilisez des algorithmes de chiffrement forts et évitez d'utiliser des algorithmes obsolètes ou faibles. Il est important de vérifier régulièrement les algorithmes utilisés et de les mettre à jour si nécessaire.
- **Utiliser des règles de sécurité strictes** : Configurez des règles de sécurité strictes pour limiter l'accès aux ressources du système. Il est important de limiter l'accès aux fichiers et répertoires sensibles.
- **Contrôle d'accès** : Mettez en place des contrôles d'accès pour limiter l'accès aux ressources du système. Il est important de définir des groupes d'utilisateurs et des rôles pour les utilisateurs, ainsi que de limiter les accès en fonction de ces rôles.
- **Mettre à jour régulièrement** : Il est important de maintenir le système à jour en installant les dernières mises à jour de sécurité et correctifs pour éviter les vulnérabilités connues.
- **Utiliser un filtrage de contenu** : Configurez un filtrage de contenu pour bloquer les demandes malveillantes et les attaques telles que les injections SQL et les attaques XSS.
- **Journalisation et surveillance** : Configurez une journalisation et une surveillance pour suivre les activités sur le système et détecter les anomalies. Cela permettra de détecter les tentatives d'intrusion et les activités suspectes.

Il est important de suivre ces étapes pour améliorer la sécurité de votre reverse proxy web et éviter les attaques potentielles. Cependant, il est important de noter que la sécurité est un processus continu et qu'il est important de maintenir le système à jour et de surveiller régulièrement les activités pour détecter les vulnérabilités et les menaces potentielles.

SEC-LEC : Durcissement sécurité Linux

Durcissement complémentaire - Durcissement des serveurs Web

La configuration SSL/TLS est essentielle pour la sécurité d'un reverse proxy web. SSL/TLS permet de chiffrer la communication entre le client et le serveur, ce qui empêche les attaques de type "man-in-the-middle" et protège les données des utilisateurs.

- Letsencrypt est un organisme qui fournit des certificats SSL/TLS gratuits, automatisés et ouverts pour les sites web. Let's Encrypt utilise le protocole ACME pour vérifier les domaines et délivrer des certificats SSL/TLS. certbot est un outil qui permet de simplifier la configuration de Let's Encrypt en automatisant la vérification des domaines et la délivrance des certificats
- SSL-config est un outil fourni par Mozilla pour aider à configurer correctement SSL/TLS sur un serveur web. SSL Config fournit des recommandations pour les protocoles, les algorithmes de chiffrement, les certificats et les en-têtes HTTP de sécurité. SSL Config fournit des fichiers de configuration pour Apache, Nginx, et d'autres serveurs web
- SSLLABS est un service fourni par Qualys qui permet de tester la configuration SSL/TLS d'un site web. SSL Labs fournit un rapport détaillé sur les protocoles, les algorithmes de chiffrement, les certificats et les en-têtes HTTP de sécurité utilisés par le serveur web. SSL Labs fournit également des recommandations pour améliorer la sécurité du site web

Pour configurer SSL/TLS sur un reverse proxy web, il est recommandé de suivre les recommandations de SSL Config et de tester la configuration avec SSL Labs. Pour utiliser Let's Encrypt, vous pouvez installer Certbot et suivre les instructions pour générer des certificats SSL/TLS gratuits pour votre site web. Il est important de maintenir les certificats SSL/TLS à jour et de surveiller régulièrement les rapports de SSL Labs pour détecter les vulnérabilités et les menaces potentielles.

SEC-LEC : Durcissement sécurité Linux

Durcissement complémentaire - Durcissement des serveurs Web

- ModSecurity est un pare-feu applicatif Web open-source qui peut être utilisé pour sécuriser les applications Web en détectant et en bloquant les attaques. Il s'agit d'un module Apache qui s'intègre facilement à la pile LAMP (Linux, Apache, MySQL, PHP/Python/Perl). ModSecurity peut être configuré pour bloquer les attaques les plus courantes, telles que les injections SQL, les attaques de script intersite (XSS) et les attaques de force brute.

Les règles de sécurité de ModSecurity sont appelées les règles de sécurité de base (Core Rule Set ou CRS). Les CRS sont une collection de règles de sécurité pré-configurées pour protéger les applications Web contre les attaques les plus courantes. Les CRS sont maintenues par la communauté et sont régulièrement mises à jour pour inclure de nouvelles règles de sécurité.

- Dirbuster est un outil de test de pénétration qui peut être utilisé pour détecter les répertoires et les fichiers cachés sur un site Web. DirBuster tente d'accéder à des répertoires et des fichiers connus en utilisant des dictionnaires de mots de passe et des attaques de force brute. DirBuster peut être utilisé pour tester la sécurité d'un site Web en détectant les répertoires et les fichiers qui pourraient être utilisés pour accéder aux informations sensibles ou pour lancer des attaques.

En utilisant ModSecurity avec les CRS et DirBuster, on peut améliorer considérablement la sécurité d'un reverse proxy Web. ModSecurity peut être configuré pour bloquer les attaques détectées par les CRS, tandis que DirBuster peut être utilisé pour détecter les répertoires et les fichiers cachés qui pourraient être utilisés pour lancer des attaques. Cela permet de détecter les vulnérabilités potentielles et d'empêcher les attaques avant qu'elles ne puissent causer des dommages.

Durcissement complémentaire - Durcissement des serveurs Web

Dirb, DirBuster et DirStalk sont tous des outils de découverte de répertoires et de fichiers cachés sur un site Web. Cependant, ils ont des différences significatives en termes de fonctionnalités, de méthodes et d'objectifs.

- Dirb est un outil en ligne de commande qui utilise des attaques de force brute pour découvrir les répertoires et les fichiers cachés sur un site Web. Il peut être utilisé pour détecter des vulnérabilités et des failles de sécurité sur le site. Dirb est simple à utiliser et peut être utilisé en combinaison avec d'autres outils de test de pénétration.
- DirBuster, quant à lui, est un outil graphique qui utilise des dictionnaires de mots de passe pour détecter les répertoires et les fichiers cachés sur un site Web. Il est également capable de suivre des liens pour détecter des ressources cachées supplémentaires. DirBuster est facile à utiliser, avec une interface utilisateur graphique, et peut être utilisé en conjonction avec d'autres outils de test de pénétration.
- DirStalk est un outil de découverte de répertoires qui utilise une approche différente de celle de Dirb et DirBuster. DirStalk utilise une liste de noms de fichiers et de répertoires courants pour découvrir des ressources cachées. Il est facile à utiliser et peut être configuré pour rechercher des fichiers et des répertoires spécifiques.

En résumé, Dirb, DirBuster et DirStalk sont des outils de test de pénétration pour découvrir des répertoires et des fichiers cachés sur un site Web. Dirb est axé sur l'attaque de force brute, DirBuster utilise des dictionnaires de mots de passe pour découvrir des ressources cachées, et DirStalk utilise une liste de noms de fichiers et de répertoires courants pour détecter les ressources cachées. Chaque outil peut être utilisé en fonction de l'objectif de la mission de test de pénétration.

SEC-LEC : Durcissement sécurité Linux

Durcissement complémentaire - Durcissement des serveurs mail

Le durcissement des serveurs mail consiste à mettre en place des mesures de sécurité pour protéger les serveurs de messagerie électronique contre les menaces potentielles telles que les attaques par déni de service (DoS), les attaques par force brute, les attaques par phishing, les spams et les virus.

Voici quelques mesures de sécurité courantes pour durcir un serveur mail :

- **Configuration de DNS et SPF** : Le serveur mail doit être configuré pour vérifier que le domaine d'envoi du courriel est autorisé à envoyer des courriels en utilisant la technologie SPF.
- **Utilisation d'un certificat SSL/TLS** : Le serveur mail doit utiliser un certificat SSL/TLS pour sécuriser les connexions SMTP et POP/IMAP.
- **Configuration des ports de messagerie** : Les ports SMTP, POP et IMAP doivent être configurés pour n'accepter les connexions que depuis les adresses IP autorisées.
- **Configuration du pare-feu** : Un pare-feu doit être configuré pour bloquer les connexions entrantes non autorisées.
- **Surveillance des journaux** : Les journaux du serveur mail doivent être surveillés pour détecter toute activité suspecte ou non autorisée.
- **Mise à jour régulière des logiciels** : Les logiciels utilisés sur le serveur mail doivent être mis à jour régulièrement pour corriger les failles de sécurité et les vulnérabilités.
- **Configuration des filtres anti-spam** : Des filtres anti-spam doivent être configurés pour réduire les spams et les courriels malveillants.
- **Utilisation de DKIM et DMARC** : Le serveur mail doit être configuré pour utiliser les protocoles DKIM et DMARC pour détecter les courriels falsifiés.
- **Utilisation de logiciels anti-virus et anti-malware** : Le serveur mail doit être équipé de logiciels anti-virus et anti-malware pour détecter les menaces potentielles.

Il est important de noter que la sécurité d'un serveur mail dépend de nombreux facteurs, notamment de la configuration du serveur, de l'utilisation de logiciels tiers et des pratiques de sécurité en place. Il est donc important de consulter les ressources de sécurité recommandées pour chaque serveur de messagerie électronique spécifique.

Durcissement complémentaire - Durcissement des serveurs mail

Il est important de placer, en bordure de votre réseau, un ou plusieurs MTA (Mail Transfer Agent) avec les Milter pour le spam, les virus et autres logiciels de sécurité pour vérifier les courriels entrants et sortants avant de les rediriger vers le serveur de stockage des courriels pour plusieurs raisons :

- **Réduire la charge sur le serveur de stockage de courriels** : Le traitement des courriels peut être très intensif, en particulier pour les filtres anti-spam et anti-virus. En plaçant un ou plusieurs MTA avec les filtres appropriés devant le serveur de stockage de courriels, vous pouvez réduire la charge sur le serveur de stockage de courriels et améliorer les performances.
- **Améliorer la sécurité** : En utilisant les filtres Milter pour le spam, les virus et autres logiciels de sécurité, vous pouvez améliorer la sécurité du serveur de messagerie en bloquant les courriels malveillants avant qu'ils ne soient livrés aux utilisateurs. Cela peut aider à prévenir les attaques par phishing, les logiciels malveillants et les spams.
- **Permettre la personnalisation des filtres** : En utilisant les filtres Milter, vous pouvez personnaliser les filtres anti-spam et anti-virus en fonction des besoins de votre organisation. Cela peut inclure des règles de filtrage spécifiques à votre entreprise pour améliorer la précision des filtres.
- **Faciliter la maintenance et la gestion** : En plaçant un ou plusieurs MTA avec les filtres appropriés devant le serveur de stockage de courriels, vous pouvez faciliter la maintenance et la gestion du serveur de messagerie. Les MTA sont souvent plus simples à configurer et à gérer que les serveurs de stockage de courriels, ce qui peut réduire les coûts et la complexité de la gestion du serveur de messagerie.

En somme, l'utilisation d'un ou plusieurs MTA avec les filtres Milter pour le spam, les virus et autres logiciels de sécurité est une pratique courante pour améliorer la sécurité, la performance et la gestion des serveurs de messagerie électronique.

SEC-LEC : Durcissement sécurité Linux

Durcissement complémentaire - Durcissement des serveurs FTP

A moins d'y être contraints et forcés, n'utilisez pas FTP. Jamais. Pouf, le protocole FTP a disparu.

En effet, il est préférable de privilégier l'utilisation de SFTP (Secure File Transfer Protocol) plutôt que d'utiliser FTP (File Transfer Protocol) pour transférer des fichiers entre les serveurs et les clients.

FTP est un protocole de transfert de fichiers non sécurisé qui transmet les informations d'identification et les données de manière non cryptée, ce qui peut rendre ces informations vulnérables aux attaques de type interception ou vol. De plus, FTP ne prend en charge que la gestion de l'accès en lecture et écriture aux fichiers.

En revanche, SFTP, qui est basé sur SSH (Secure Shell), utilise des clés de chiffrement pour crypter les informations d'identification et les données de transfert de fichiers. SFTP offre également une sécurité supplémentaire en fournissant des fonctionnalités d'authentification, d'intégrité et de confidentialité des données de transfert de fichiers. Il offre également une gestion de l'accès en lecture et écriture ainsi que des options pour configurer les permissions d'accès.

En plus de l'utilisation de SFTP, il est également important de suivre les bonnes pratiques de sécurité pour les serveurs, telles que la configuration d'un pare-feu pour limiter l'accès au serveur, l'installation de mises à jour de sécurité régulières, la gestion des comptes utilisateurs avec des mots de passe forts et l'utilisation de la surveillance et des journaux de sécurité pour détecter les tentatives d'intrusion.

En somme, **privilégier l'utilisation de SFTP plutôt que l'utilisation de FTP non sécurisé** est une mesure importante pour renforcer la sécurité des transferts de fichiers entre les serveurs et les clients.

SEC-LEC : Durcissement sécurité Linux

Durcissement complémentaire - Durcissement Applicatif

Le durcissement applicatif est une pratique visant à renforcer la sécurité des applications en les protégeant contre les attaques et les vulnérabilités.

Voici quelques pratiques courantes pour durcir les applications :

- **Validation des entrées utilisateur** : Les entrées utilisateur doivent être validées pour éviter les attaques d'injection de code. Cela implique de s'assurer que les données saisies par l'utilisateur sont conformes à des critères spécifiques, tels que la longueur, le format et le type de données attendues
- **Limitation des privilèges d'accès** : Les applications ne doivent avoir que les privilèges d'accès nécessaires pour effectuer leurs tâches. Les utilisateurs et les processus doivent avoir des autorisations minimales pour éviter les attaques de type élévation de privilèges
- **Protection des données sensibles** : Les données sensibles telles que les mots de passe, les informations personnelles ou les données financières doivent être protégées à l'aide de techniques de cryptage et de hachage pour éviter les violations de données
- **Gestion des erreurs** : Les erreurs doivent être gérées de manière sécurisée pour éviter la divulgation d'informations sensibles ou l'exposition de vulnérabilités
- **Éloignement de la bordure du réseau** : Les applications doivent être conçues de manière à être placées loin de la bordure du réseau, c'est-à-dire qu'elles ne doivent pas être directement exposées à Internet. Elles doivent être placées derrière un pare-feu et un proxy pour bloquer les tentatives d'attaques et de piratages. Cela peut être réalisé en utilisant des architectures de réseau telles que DMZ (zone démilitarisée) ou en plaçant l'application derrière un serveur proxy

SEC-LEC : Durcissement sécurité Linux

Durcissement complémentaire - Durcissement Applicatif

- **Exportation des données spécifiques de l'application** : Les données spécifiques de l'application doivent être exportées régulièrement dans un but de sauvegarde. Cela permet de récupérer les données en cas de panne du système ou de cyberattaque. Les sauvegardes doivent être stockées sur un serveur distant sécurisé et ne doivent être accessibles qu'aux personnes autorisées
- **Sécurisation des communications** : Les communications entre l'application et les utilisateurs ou les serveurs tiers doivent être sécurisées à l'aide de protocoles cryptés tels que HTTPS ou SSL/TLS
- **Mise à jour régulière** : Les applications doivent être mises à jour régulièrement pour corriger les vulnérabilités connues et les failles de sécurité.
- **Tests de pénétration** : Les tests de pénétration doivent être effectués régulièrement pour identifier les vulnérabilités de l'application et s'assurer qu'elle est suffisamment sécurisée
- **Formation des utilisateurs** : Les utilisateurs de l'application doivent être formés à la sécurité informatique pour éviter les erreurs humaines pouvant entraîner des violations de données ou des compromissions de sécurité

En appliquant ces pratiques, les développeurs et les administrateurs peuvent aider à renforcer la sécurité des applications et à protéger les données sensibles des utilisateurs.

SEC-LEC : Durcissement sécurité Linux

Durcissement complémentaire - Durcissement Des hyperviseurs

Le durcissement des hyperviseurs est une étape importante pour garantir la sécurité de l'infrastructure de virtualisation. Les hyperviseurs sont des couches de virtualisation qui permettent l'exécution de plusieurs machines virtuelles sur une seule machine physique.

Voici quelques pratiques courantes pour le durcissement des hyperviseurs :

- **Installer les mises à jour de sécurité** : Les mises à jour de sécurité doivent être installées régulièrement sur l'hyperviseur pour s'assurer qu'il est protégé contre les dernières vulnérabilités.
- **Désactiver les fonctionnalités inutiles** : Les fonctionnalités inutiles doivent être désactivées sur l'hyperviseur pour réduire la surface d'attaque. Les fonctionnalités qui ne sont pas nécessaires pour l'environnement de virtualisation doivent être désactivées ou supprimées.
- **Restreindre l'accès au système d'exploitation de l'hyperviseur** : L'accès au système d'exploitation de l'hyperviseur doit être restreint uniquement aux personnes autorisées. Les comptes d'administrateur doivent être protégés avec des mots de passe forts et ne doivent pas être partagés.
- **Configurer le pare-feu** : Un pare-feu doit être configuré sur l'hyperviseur pour bloquer les connexions non autorisées.
- **Surveiller l'activité de l'hyperviseur** : L'activité de l'hyperviseur doit être surveillée pour détecter les tentatives d'attaque ou les comportements anormaux. Les journaux d'événements de l'hyperviseur doivent être surveillés en temps réel pour identifier les incidents de sécurité.

SEC-LEC : Durcissement sécurité Linux

Durcissement complémentaire - Durcissement Des hyperviseurs

- **Isoler les machines virtuelles** : Les machines virtuelles doivent être isolées les unes des autres pour minimiser les risques d'attaques croisées. Les machines virtuelles qui n'ont pas besoin de communiquer entre elles ne doivent pas être connectées au même réseau.
- **Désactivation des périphériques non nécessaires** : Il est important de désactiver les périphériques virtuels qui ne sont pas nécessaires dans les machines virtuelles, comme les lecteurs de disquettes virtuels, les ports série ou parallèle virtuels, etc.
- **Utilisation d'un profil de sécurité** : Les hyperviseurs modernes tels que Xen et KVM permettent l'utilisation de profils de sécurité, tels qu'AppArmor ou SELinux, pour limiter les actions que les machines virtuelles peuvent effectuer.
- **Activation du PCI Passthrough/IOMMU** : Cette fonctionnalité permet de donner l'accès direct à un périphérique physique à une machine virtuelle, en contournant l'hyperviseur. Cela peut être utile pour les applications qui nécessitent des performances élevées ou une latence faible.
- **Restriction de l'accès réseau** : L'hyperviseur doit être configuré pour limiter l'accès réseau des machines virtuelles, en bloquant les ports non utilisés et en limitant l'accès aux ressources réseau.

En appliquant ces pratiques, les administrateurs peuvent renforcer la sécurité de l'hyperviseur et réduire les risques d'attaques et de pertes de données.

SEC-LEC : Durcissement sécurité Linux

Durcissement complémentaire - Durcissement Des VM

Le durcissement des VMs est similaire à celui d'un serveur physique, mais il y a quelques différences à prendre en compte en raison de la nature virtuelle des machines.

Voici quelques mesures de durcissement spécifiques à prendre en compte pour les VMs :

- **Configuration du réseau** : Lors de la configuration du réseau d'une machine virtuelle, il est important de s'assurer que l'accès au réseau est limité aux ports nécessaires uniquement, et que les ports inutilisés sont bloqués.
- **Sécurité de l'hyperviseur** : Comme les machines virtuelles s'exécutent sur l'hyperviseur, il est important de sécuriser l'hyperviseur lui-même. Les mesures de sécurité de l'hyperviseur incluent la mise à jour régulière, la configuration appropriée des autorisations et l'application de contrôles d'accès.
- **Isolation** : Les machines virtuelles doivent être isolées les unes des autres, afin d'éviter que des attaquants ne puissent s'infiltrer d'une machine virtuelle à une autre. Les mesures d'isolation comprennent l'utilisation de réseaux virtuels distincts, la limitation des autorisations et la configuration des paramètres de sécurité de l'hyperviseur.
- **Isoler les VMs de l'hyperviseur** : Ne pas laisser passer de trafic entre eux. Cela permet de réduire les risques de compromission d'une VM qui pourrait ensuite être utilisée pour attaquer l'hyperviseur ou les autres VMs.
- **Aucune VM ne se trouve sur le réseau de management de l'hyperviseur :** Afin d'empêcher les attaquants potentiels d'exploiter une faille de sécurité dans la VM pour compromettre l'hyperviseur.
- **Surveillance des activités** : Les machines virtuelles doivent être surveillées régulièrement pour détecter toute activité suspecte. Les outils de surveillance comprennent les journaux d'événements, les outils de surveillance des performances et les outils de détection des menaces.
- **Sauvegardes régulières** : Les machines virtuelles doivent être sauvegardées régulièrement pour assurer la disponibilité des données en cas de sinistre ou d'incident de sécurité.

En résumé, le durcissement des VMs est similaire à celui d'un serveur physique, mais nécessite des mesures de sécurité spécifiques pour protéger l'hyperviseur et assurer l'isolation entre les machines virtuelles.

SEC-LEC : Durcissement sécurité Linux

Durcissement complémentaire - Durcissement IPv6

Le durcissement d'IPv6 sous Linux peut être réalisé en prenant en compte les mesures de sécurité suivantes :

- **Désactiver les interfaces IPv6 non utilisées** : cela permet de réduire la surface d'attaque en limitant l'accès aux interfaces réseau qui ne sont pas nécessaires.
- **Utiliser les filtres de pare-feu** : les filtres de pare-feu permettent de contrôler le trafic réseau entrant et sortant en fonction des règles définies. Cela peut aider à bloquer les attaques en bloquant le trafic malveillant.
- **Configurer correctement les paramètres d'adressage** : il est important de configurer correctement les paramètres d'adressage IPv6 pour éviter les adresses d'interface basées sur le temps et empêcher les adresses de se répéter.
- **Utiliser des adresses IPv6 sécurisées** : il est recommandé d'utiliser des adresses IPv6 temporaires qui changent régulièrement pour éviter la surveillance ou la reconnaissance.

Enfin, il est important de noter que l'IPv6 doit être utilisé sur Internet car il est conçu pour remplacer l'IPv4 obsolète, qui a atteint sa limite d'adresses. L'IPv6 est plus sûr et plus fiable que l'IPv4, ce qui le rend indispensable pour l'avenir d'Internet.

SEC-LEC : Durcissement sécurité Linux

Durcissement complémentaire

Lynis est un outil open source d'audit de sécurité pour les systèmes Unix et Linux. Il est conçu pour effectuer des analyses de sécurité approfondies des systèmes et des réseaux et pour fournir des recommandations pour améliorer la sécurité globale.

Lynis effectue une vérification des systèmes en utilisant des tests automatisés et des règles de conformité pour déterminer les vulnérabilités potentielles et les risques de sécurité. Les tests incluent la vérification des permissions de fichiers, la configuration du pare-feu, la configuration des services réseau, la vérification des mises à jour de sécurité et bien plus encore.

Lynis est facile à installer et à utiliser, et il peut être exécuté à partir de la ligne de commande. Il fournit un rapport détaillé après chaque exécution, qui comprend les résultats des tests, les recommandations de sécurité et des conseils pour améliorer la sécurité du système.

Lynis est utilisé par de nombreux professionnels de la sécurité informatique, y compris les administrateurs de système, les auditeurs de sécurité et les consultants en sécurité. Il est régulièrement mis à jour pour inclure de nouveaux tests de sécurité et pour s'assurer qu'il reste un outil de sécurité précis et fiable pour les systèmes Unix et Linux.

SEC-LEC : Durcissement sécurité Linux

Durcissement complémentaire

Pour installer Lynis sur une distribution Linux qui utilise APT (comme Ubuntu, Debian ou Linux Mint), vous pouvez suivre ces étapes :

- Tapez la commande suivante pour installer Lynis : *sudo apt install lynis*
- Une fois l'installation terminée, vous pouvez lancer Lynis en tapant la commande : *sudo lynis audit system*.

Cette commande permet de lancer une analyse de sécurité du système.

- Lorsque l'analyse est terminée, Lynis affiche un rapport de sécurité détaillé qui comprend les résultats des tests effectués et les recommandations de sécurité pour améliorer la sécurité de votre système.

Il est important de noter que l'exécution de Lynis nécessite des privilèges root pour accéder aux fichiers système et effectuer les tests de sécurité. Par conséquent, il est recommandé de l'exécuter en tant que superutilisateur en utilisant la commande sudo.

Il est également recommandé de régulièrement exécuter Lynis pour s'assurer que le système est toujours sécurisé et pour détecter les nouvelles vulnérabilités potentielles.

SEC-LEC : Durcissement sécurité Linux

Durcissement complémentaire

Ca ressemble à ceci :

```
 +] SSH Support
------------------------------------
  - Checking running SSH daemon                               [ FOUND ]
    - Searching SSH configuration                             [ FOUND ]
    - OpenSSH option: AllowTcpForwarding                      [ SUGGESTION ]
    - OpenSSH option: ClientAliveCountMax                     [ SUGGESTION ]
    - OpenSSH option: ClientAliveInterval                     [ OK ]
```

Puis finalement à ceci :

```
  * Determine if protocol 'tipc' is really needed on this system [NETW-3200]
      https://cisofy.com/lynis/controls/NETW-3200/

  * Check iptables rules to see which rules are currently not used [FIRE-4513]
      https://cisofy.com/lynis/controls/FIRE-4513/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : AllowTcpForwarding (set YES to NO)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : ClientAliveCountMax (set 3 to 2)
      https://cisofy.com/lynis/controls/SSH-7408/

  * Consider hardening SSH configuration [SSH-7408]
    - Details  : Compression (set YES to NO)
      https://cisofy.com/lynis/controls/SSH-7408/
```

SEC-LEC : Durcissement sécurité Linux

Durcissement complémentaire

Checksec est un outil open source qui permet de vérifier les mesures de sécurité prises sur les fichiers binaires exécutables sur Linux. L'outil permet de vérifier les options de sécurité telles que la protection de la pile, la randomisation de l'espace d'adressage (ASLR) et l'exécution de code non autorisé (NX).

Voici les étapes pour installer et utiliser Checksec sur le fichier binaire exécutable /usr/bin/kvm :

- Installez Checksec en utilisant la commande suivante : *sudo apt install checksec*
- Utilisez la commande checksec --file=/usr/bin/kvm pour vérifier les mesures de sécurité prises sur le binaire exécutable KVM

La commande checksec affichera un rapport détaillé qui comprendra les options de sécurité activées ou désactivées pour le binaire exécutable KVM. Les options de sécurité incluent notamment la randomisation de l'espace d'adressage (ASLR), la protection de la pile, l'exécution de code non autorisé (NX), la protection contre les attaques par débordement de tampon et la protection contre les liens dynamiques non sécurisés.

```
$ sudo checksec --file=/usr/bin/kvm
RELRO           STACK CANARY      NX            PIE             RPATH      RUNPATH    Symbols    FORTIFY    Fortified    Fortifiable    FILE
Full RELRO      Canary found      NX enabled    PIE enabled     No RPATH   No RUNPATH   No Symbols   Yes    15    36    /usr/bin/kvm
```

Il est recommandé d'utiliser Checksec régulièrement pour vérifier les mesures de sécurité prises sur les fichiers binaires exécutables sur votre système, afin de s'assurer que votre système est correctement sécurisé.

Des Questions