|  |  |  |
| --- | --- | --- |
| tripwire  http://upload.wikimedia.org/wikipedia/commons/thumb/3/35/Tux.svg/512px-Tux.svg.png  tripwire (suite)  http://upload.wikimedia.org/wikipedia/commons/thumb/3/35/Tux.svg/512px-Tux.svg.png  tripwire (suite)  http://upload.wikimedia.org/wikipedia/commons/thumb/3/35/Tux.svg/512px-Tux.svg.png  tripwire (suite)  http://upload.wikimedia.org/wikipedia/commons/thumb/3/35/Tux.svg/512px-Tux.svg.png  tripwire (suite)  http://upload.wikimedia.org/wikipedia/commons/thumb/3/35/Tux.svg/512px-Tux.svg.png  tripwire (suite)  http://upload.wikimedia.org/wikipedia/commons/thumb/3/35/Tux.svg/512px-Tux.svg.png  tripwire (suite)  http://upload.wikimedia.org/wikipedia/commons/thumb/3/35/Tux.svg/512px-Tux.svg.png |  | Protection des fichiers sensibles  *tripwire* est un logiciel permettant de s'assurer que les fichiers sensibles sur un ordinateur ne sont pas modifiés sans que cela ne déclenche une alerte.  Pour ce faire, le logiciel crée une base de données contenant la signature numérique des fichiers que l'administrateur souhaite surveiller. Lors de la phase de contrôle d'intégrité, *tripwire* recalcule la signature numérique de chacun des fichiers à surveiller et vérifie que cette signature correspond bien à celle calculée lors de la création de la base de données. Si les deux signatures ne correspondent pas, *tripwire* émet alors une alerte.  Les fichiers à surveiller peuvent être classés selon différents degrés de criticité. *tripwire* peut être assez complexe à configurer car son objectif de sécurité entraîne un chiffrement des fichiers utilisés par l'outil lui-même. Les fichiers de configuration de *tripwire* sont chiffrés, la base de données peut (doit) aussi être chiffrée afin d'éviter que ce soit la base qui soit altérée en dehors du contrôle de l'administrateur.  En conséquence, chaque nouveau réglage entraîne un re-chiffrement des fichiers de configuration et de la base de données.  Les éventuelles alertes à la suite de modifications de fichiers peuvent être transmises par courriel, ce qui évite que ce soit le rapport du contrôle qui soit intercepté.  Installation  L’installation se fait depuis les dépôts …  # **apt-get install tripwire**  Les différents fichiers, suite à l’installation, se retrouvent dans */etc/tripwire*, dans */var/lib/tripwire* et dans */usr/sbin* pour les exécutables.  Configuration  De manière standard, on trouve les fichiers de configuration dans */etc/tripwire*.  Deux configurations sont à modifier selon ses besoins.  Elles ont chacune une version accessible en clair …   * */etc/tripwire/twcfg.txt* Fichier qui est propre à la configuration du service en lui-même ; * */etc/tripwire/twpol.txt* Fichier qui concerne les politiques à mettre en place.   Respectivement, une fois configurés, ces fichiers deviendront …   * */etc/tripwire/tw.cfg* pour la configuration du service  et * */etc/tripwire/tw.pol* pour la spécification des stratégies (*policies*).               La configuration du service est stockée dans le fichier */etc/tripwire/tw.cfg*, qui est une version modifiée du */etc/tripwire/twcfg.txt*. Cette dernière est à moduler selon ses besoins.  Elle contient notamment le nom et l’emplacement de la base de données où *tripwire* va loger tous ses fichiers.  **La configuration des startégies (*policies*)**  Comme première vérification …  # **nano /etc/tripwire/twpol.txt**  C’est un fichier texte, à la syntaxe très particulière. Pas mal de stratégies sont déjà à sa disposition, implémentées ou commentées d’ailleurs, et cela permet de se familiariser avec la syntaxe.  Si on veut faire dans le spécifique, il est possible de rajouter à la fin de la configuration …  *rulename = "Application to monitor",*  *severity = 100,*  *emailto = lsavard@cmaisonneuve.qc.ca*  */APPS -> $(IgnoreNone)-MCHracm (recurse=true) ;*  Après avoir défini la stratégie dans le fichier twpol.txt, lancer la commande suivante :  # **twadmin -m P -c /etc/tripwire/tw.cfg -S /etc/tripwire/site.key /etc/tripwire/twpol.txt**  *Please enter your site passphrase:*  *Wrote policy file: /etc/tripwire/tw.pol*  **-m P équivaut également à –create-polfile.**  Maintenant que les fichiers de configurations sont complétés, on doit créer la base des sceaux de référence.  # **tripwire --init -c /etc/tripwire/tw.cfg**  *Parsing policy file: /etc/tripwire/tw.pol*  *Generating the database...*  *\*\*\* Processing Unix File System \*\*\**  *Wrote database file: /var/lib/tripwire/db.twd*  *The database was successfully generated.*  Note …  Il est possible que la commande génère des erreurs en fonction du système d’exploitation et des services installés.  La base de données créée, il ne reste plus qu’à rentrer les valeurs de référence en lançant le fameux check.  # **tripwire --check**  *Parsing policy file: /etc/tripwire/tw.pol*  *\*\*\* Processing Unix File System \*\*\**  *Performing integrity check...*  *Wrote report file: /var/lib/tripwire/report/****abc****.twr*  *Total objects scanned: 52397*  *Total violations found: 0*  Notes …  Il est possible que la commande génère des erreurs en fonction du système d’exploitation et des services installés.  *abc* dans le nom du fichier varie selon l’hôte.  Les rapports produits par les check de *tripwire* sont situés par défaut sous */var/lib/tripwire/report/* et ont une extension en *.twr*. Ce sont des data qui sont lisibles via la commande *twprint*. De là, il est facile de rediriger la sortie standard vers un fichier lisible via un less par exemple, c’est à votre convenance.  # **twprint -m r -r /var/lib/tripwire/report/abc.twr**  Notes …  Il est possible que la commande génère des erreurs en fonction du système d’exploitation et des services installés.  *abc* dans le nom du fichier varie selon l’hôte.  Évolution de la base et mise à jour des stratégies  Comme les systèmes de fichiers évoluent vite avec les mises à jour, il est nécessaire de faire évoluer la base de données de *tripwire* en conséquence.  Tout d’abord, on doit mettre à jour la base de données de *tripwire* à l’aide du rapport en question …  # **tripwire -m u --twrfile /var/lib/tripwire/report/abc.twr**  *Please enter your local passphrase:*  *Wrote database file: /var/lib/tripwire/db.twd*  Note …  *abc* dans le nom du fichier varie selon l’hôte.  Si besoin, il est possible de revoir les stratégies.  Pour cela, il faut générer à nouveau le fihcier *tw.pol* après avoir modifier le fichier *twpol.txt* …  # **twadmin -m P -c /etc/tripwire/tw.cfg -S /etc/tripwire/site.key /etc/tripwire/twpol.txt**  *Please enter your site passphrase:*  *Wrote policy file: /etc/tripwire/tw.pol*  Il faut par la suite supprimer et recréer la database.  # **rm /var/lib/tripwire/db.twd**  # **tripwire --init -c /etc/tripwire/tw.cfg**  Automatiser le tout  tripwire n’est pas un service (daemon) et il est nécessaire de le lancer de façon récurrente.  crond s’impose donc …  *00 03 \* \* \* /usr/sbin/tripwire --check*  Tout est prêt pour avertir dès qu’une modification est faite sur un des éléments sous surveillance.  Conclusion  tripwire est une réponse à un besoin élémentaire en terme de sécurité. Bien qu’elle nécessite un petit ajustement dans sa prise en main et une maintenance continue, elle reste plus que pertinente.  Références  <https://fr.wikipedia.org/wiki/Tripwire_%28logiciel%29> <http://www.k-tux.com/tripwire-controle-dintegrite-et-monitoring> |
|  |  |  |