INSTALLATION DE TRIPWIRE SOUS RASPBERRY PI

Raspberry Pi - Debian Buster Configuration de base

Tutoriel TRIPWIRE - RASPBERRY PI

David GOÏTRÉ

Table des matières

Introduction1
1. Pré requis1
2. Paramétrage du serveur
3. Paramétrage de connexion au serveur
4. Installation de Tripwire
5. Configuration de Tripwire5
6. Gestion de la base de données Tripwire6
7. Vérification des identifiants Tripwire9
8. Automatisation du rapport Tripwire10
9. Consultation du rapport11
10. Commandes RaspberryPi11
11. Conclusion

Introduction

Tripwire est un système de détection d'intrusion Linux gratuit et open-source. Il est utilisé pour détecter et signaler toute modification non autorisée des fichiers et des répertoires sous Linux. Il vous enverra également une alerte par e-mail sur les changements de fichiers/répertoires. Tripwire fonctionne en comparant l'état actuel du système de fichiers à un état de base connu et signale s'il détecte des changements.

1. Pré requis

On a besoin des différents matériels et logiciels pour la création d'un Serveur **Tripwire** avec un RaspberryPi.

- Un ou des PC client sous Windows
- Une Box (Free, Orange, Sfr...)
- Un Raspberry 3B+ avec l'OS Raspian Buster installé avec Etcher
- Un mot de passe root doit être configuré sur le serveur
- Le logiciel Putty pour se connecter en SSH au serveur VPN
- Connaitre l'interface réseau (eth0, br0, ens3...) via la commande : ip a Pour notre test c'est l'interface eth0 qui sera utilisée

Package configuration

Tripwire Configuration

Tripwire uses a pair of keys to sign various files, thus ensuring their unaltered state. By accepting here, you will be prompted for the passphrase for the first of those keys, the site key, during the installation. You are also agreeing to create a site key if one doesn't exist already. Tripwire uses the site key to sign files that may be common to multiple systems, e.g. the configuration & policy files. See twfiles(5) for more information.

Unfortunately, due to the Debian installation process, there is a period of time where this passphrase exists in a unencrypted format. Were an attacker to have access to your machine during this period, he could possibly retrieve your passphrase and use it at some later point.

If you would rather not have this exposure, decline here. You will then

<0k>

Voici la première interface que l'on doit obtenir une fois l'installation de Tripwire lancée

2. Paramétrage du serveur

Avant d'aller plus loin, il nous faut connaître l'interface réseau de notre serveur **RaspberryPI** et lui attribuer une adresse IP fixe.

a) Lister les interfaces

\$ ip link | awk '{ print \$2}' # liste les interfaces # ethtool <interface> | grep detected # détecte l'interface connectée

b) Définir une adresse IP fixe

nano /etc/network/interfaces # ouvre le fichier des interfaces

c) Copier le texte ci-dessous dans le fichier interfaces

Interface reseau de bouclage auto lo iface lo inet loopback # Interface reseau principale allow-hotplug eth0 iface eth0 inet static address 192.xxx.xxx netmask 255.255.255.0 gateway 192.xxx.xxx

d) Comme on utilise pas le dhcpcd.conf pour avoir une @IP fixe, il faut le désactiver

sudo systemctl stop dhcpcd# sudo systemctl disable dhcpcd# sudo reboot

e) Rebooter le serveur

/etc/init.d/networking restart
reboot

f) Paramétrer le serveur

\$ raspi-config # ouvre l'utilitaire, sélectionner le menu System Options

 Raspberry Pi Software Configuration Tool (raspi-config)

 1 System Options
 Configure system settings

 2 Display Options
 Configure display settings

Sélectionner le menu **S3 Password** pour modifier le mot de passe et **S4 Hostname** pour modifier le nom du serveur.

	Deenharry Di Soft	ware Configuration Tool (raspi-config)
	Raspberry Fr SOIG	ware configuration foor (faspi-config)
C 2	114 ma 1 a a a 7 7 7 7	Pater COTD and an embrance
SI	Wireless LAN	Enter SSID and passphrase
52	Audio	Select audio out through HDMT or 3 5mm jack
02	Hudio	Screet addre through manif or 5.5mm Jack
S3	Password	Change password for the 'pi' user
S4	Hostname	Set name for this computer on a network
		-

3. Paramétrage de connexion au serveur

a) Une fois installé, ouvrir la page avec **@IPduServeur** dans le navigateur pour effectuer la configuration initiale et apprendre à configurer les appareils pour utiliser **Tripwire**. On n'a pas besoin de lancer quoi que ce soit de manière explicite, le service Tripwire est déjà démarré après l'installation.

b) Activer le **SSH** sur le serveur. Pour ce faire, ouvrir le dossier **Boot**, de la carte SD du RaspberryPi via l'explorateur de Windows et créer un fichier **ssh** (sans extension) dans ce **dossier**.

c) Ouvrir Putty et se connecter au serveur Tripwire avec les identifiants (par défaut pi/raspberry)

b) Mettre à jour les packages du système vers la dernière version. Exécuter la commande suivante pour mettre à jour et mettre à niveau les packages de votre système :

sudo apt update -y
sudo apt upgrade -y

4. Installation de Tripwire

Par défaut, le paquet Tripwire n'est pas disponible dans le référentiel par défaut Debian 10. Il faut l'installer avec la commande suivante :

sudo apt install tripwire -y

Tripwire utilise deux clés différentes pour l'authentification et le cryptage des fichiers.

La **clé locale** est utilisée pour protéger les fichiers spécifiques à la machine locale, tels que la base de données Tripwire. La clé locale peut également être utilisée pour signer des rapports de contrôle d'intégrité.

La **clé de site** est utilisée pour protéger les fichiers qui pourraient être utilisés sur plusieurs systèmes. Cela inclut les fichiers de stratégie et de configuration.

Attention ces deux passphrases ne sont pas stockées. Il est donc nécessaire de les enregistrer dans un espace de stockage externe.

	Tripwire Con	ofiguration
Tripwire uses a pair of keys to s the passphrase for the first of t doesn't exist already. Tripwire policy files. See twfiles(5) for	ign various files, thus ensuring the hose keys, the site key, during the uses the site key to sign files that more information.	eir unaltered state. By accepting here, you will be prompted for installation. You are also agreeing to create a site key if one may be common to multiple systems, e.g. the configuration &
Unfortunately, due to the Debian Were an attacker to have access t point.	installation process, there is a per o your machine during this period, h	iod of time where this passphrase exists in a unencrypted format. The could possibly retrieve your passphrase and use it at some later
If you would rather not have this hand. See twadmin(8) for more in	exposure, decline here. You will formation.	then need to create a site key, configuration file & policy file by
Do you wish to create/use your si	te key passphrase during installatio	an?
	syes	<no></no>

a) Cliquer sur le bouton Yes pour créer la phrase secrète de la clé de site

b) Sélectionner Yes et appuyer sur la touche Enter pour reconstruire le fichier de configuration Tripwire



c) Sélectionner Yes et appuyer sur la touche Enter pour reconstruire le fichier de politique Tripwire

Tripwire Cont	iguration			
Tripwire keeps its policies on what attributes of which files should be default, from /etc/tripwire/twpol.txt	be monitored in a encrypted database that is generated, by			
Any changes to /etc/tripwire/twpol.txt, either as a result of a change regeneration of the encrypted database before they will take effect.	e in this package or due to administrator activity, require the			
Selecting this action will result in your being prompted for the site key passphrase during the post-installation process of this package.				
Rebuild Tripwire policy file?				
Steel State	<no></no>			

d) Saisir le mot de passe de clé de site et cliquer sur le bouton Ok (ex : tripsite)

Get site passphrase
Tripwire uses two different keys for authentication and encryption of files. The site key is used to protect files that could be used across several systems. This includes the policy and configuration files.
You are being prompted for this passphrase either because no site key exists at this time or because you have requested the rebuilding of the policy or configuration files.
Remember this passphrase; it is not stored anywhere!
Enter site-key passphrase:

e) Saisir le mot de passe de clé local et cliquer sur le bouton Ok (ex : triplocal)

Get local passphrase
Tripwire uses two different keys for authentication and encryption of files. The local key is used to protect files specific to the local machine, such as the Tripwire database. The local key may also be used for signing integrity check reports.
You are being prompted for this passphrase because no local key file currently exists.
Remember this passphrase; it is not stored anywhere!
Enter local key passphrase:
Get local passphrase
Tripwire has been installed
The Tripwire binaries are located in /usr/sbin and the database is located in /var/lib/tripwire. It is strongly advised that these locations be stored on write-protected media (e.g. mounted RO floppy). See /usr/share/doc/tripwire/README.Debian for details.

<0k>

5. Configuration de Tripwire

Ensuite, on doit générer des clés **Tripwire** et initialiser la base de données. Tout d'abord, ouvrir le dossier **Tripwire** et lister le contenu

a) Ouvrir le dossier et lister toutes les clés et tous les fichiers

cd /etc/tripwire/
ls

Le résultat suivant, doit s'afficher

raspberrypi-local.key site.key tw.cfg twcfg.txt tw.pol twpol.txt

b) Ensuite, modifier le fichier de configuration Tripwire et définir REPORTLEVEL sur 4

sudo nano /etc/tripwire/twcfg.txt

c) Modifier **la ligne** et enregistrer le fichier REPORTLEVEL =4

d) Générer un nouveau fichier de configuration

sudo twadmin -m F -c tw.cfg -S site.key twcfg.txt

e) Il vous sera demandé de fournir la passphrase du site

Please enter your site passphrase: Wrote configuration file: /etc/tripwire/tw.cfg

f) Créer le fichier **twpolmake.pl** pour optimiser la politique Tripwire.

```
# sudo nano twpolmake.pl
```

```
Saisir le texte ci-dessous dans le nouveau fichier
 #!/usr/bin/perl
 $POLFILE=$ARGV[0];
 open(POL,"$POLFILE") or die "open error: $POLFILE" ;
 my($myhost,$thost);
 my($sharp,$tpath,$cond);
 my(\$INRULE) = 0;
 while () {
  chomp;
  if (($thost) = /^HOSTNAME\s*=\s*(.*)\s*;/) {
    $myhost = `hostname` ; chomp($myhost) ;
    if ($thost ne $myhost) {
      $_="HOSTNAME=\"$myhost\";";
    }
  }
  elsif ( /^{/ ) {
    $INRULE=1;
  }
  elsif ( /^}/ ) {
```

```
$INRULE=0;
 }
 elsif (\$INRULE == 1 and (\$harp,\$tpath,\$cond) = /^(\s*\#?\s*)(\/\S+)\b(\s+->\s+.+)$/) {
   ret = (\$harp = \ s/\ \#//g);
   if ($tpath eq '/sbin/e2fsadm') {
      $cond =~ s/;\s+(tune2fs.*)$/; \#$1/;
   }
   if (! -s $tpath) {
     $ = "$sharp#$tpath$cond" if ($ret == 0);
   }
   else {
      $ = "$sharp$tpath$cond";
   }
 }
 print "$ \n";
}
close(POL);
```

g) Créer le fichier de configuration

sudo perl twpolmake.pl twpol.txt > twpol.txt.new # sudo twadmin -m P -c tw.cfg -p tw.pol -S site.key twpol.txt.new

Le résultat suivant doit s'afficher

Please enter your site passphrase: Wrote policy file: /etc/tripwire/tw.pol

6. Gestion de la base de données Tripwire

Tripwire fonctionne avec une base de données, il faut donc la créer.

a) Créer la **base de données**

sudo tripwire -m i -s -c tw.cfg

Le résultat suivant doit s'affichier

Please enter your local passphrase: ### Warning: File system error. ### Filename: /var/lib/tripwire/raspberrypi.twd ### No such file or directory ### Continuing...

b) Afficher la base de données générée

sudo twprint -m d -d /var/lib/tripwire/raspberrypi.twd

Le résultat suivant doit s'afficher (voici les dernières lignes)

Object name: /var/run

Property:	Value:
Object Type	Symbolic Link
Device Number	45826
Inode Number	300433
Mode	Irwxrwxrwx
Num Links	1
UID	root (0)
GID	root (0)
Object name:	/var/tmp
Property:	Value:
Object Type	Directory
Mode	drwxrwxrwt
UID	root (0)
GID	root (0)

*** End of database ***

Open Source Tripwire 2.4 Portions copyright 2000-2018 Tripwire, Inc. Tripwire is a registered trademark of Tripwire, Inc. This software comes with ABSOLUTELY NO WARRANTY; for details use --version. This is free software which may be redistributed or modified only under certain conditions; see COPYING for details. All rights reserved.

c) Mise à jour de la base de données

sudo tripwire --update --accept-all

Le résultat suivant doit s'afficher

Error: File could not be opened. ### Filename: /var/lib/tripwire/raspberrypi.twr ### No such file or directory ### Continuing...

sudo tripwire -m c -s -c /etc/tripwire/tw.cfg

Le résultat suivant doit s'afficher (voici les dernières lignes)

"/proc/4555/net/ip mr vif" "/proc/4555/net/mcfilter6" "/proc/4555/net/rt6_stats" "/proc/4555/net/sockstat6" "/proc/4555/net/ip6_mr_vif" "/proc/4555/net/ipv6_route" "/proc/4555/net/ip_mr_cache" "/proc/4555/net/fib triestat" "/proc/4555/net/ip6_mr_cache" "/proc/4555/net/softnet_stat" "/proc/4555/net/ip6 flowlabel" "/proc/4555/net/ip_tables_names" "/proc/4555/net/ip_tables_matches" "/proc/4555/net/ip_tables_targets" "/proc/4555/net/snmp" "/proc/4555/net/wireless" "/proc/4555/net/ipconfig" "/proc/4555/net/ipconfig/ntp_servers" "/proc/4555/net/netfilter" "/proc/4555/net/netfilter/nf log" "/proc/4555/net/bnep" "/proc/4555/net/rfcomm" "/proc/4555/sched" "/proc/4555/io" "/proc/4555/cwd" "/proc/4555/maps" "/proc/4555/exe" "/proc/4555/comm" "/proc/4555/attr" "/proc/4555/attr/current" "/proc/4555/attr/prev" "/proc/4555/attr/exec" "/proc/4555/attr/fscreate" "/proc/4555/attr/keycreate" "/proc/4555/attr/sockcreate" "/proc/4555/attr/apparmor" "/proc/4555/attr/apparmor/current" "/proc/4555/attr/apparmor/prev" "/proc/4555/attr/apparmor/exec" "/proc/4555/mem"

*** End of report ***

Open Source Tripwire 2.4 Portions copyright 2000-2018 Tripwire, Inc. Tripwire is a registered trademark of Tripwire, Inc. This software comes with ABSOLUTELY NO WARRANTY; for details use --version. This is free software which may be redistributed or modified only under certain conditions; see COPYING for details. All rights reserved.

e) Afficher les fichiers de rapport Tripwire

sudo ls /var/lib/tripwire/report/

Le résultat suivant doit s'afficher

raspberrypi-20230305-194905.twr

f) Vérifier le rapport

sudo twprint -m r -t 4 -r /var/lib/tripwire/report/raspberrypi-20230305-194905.twr

7. Vérification des identifiants Tripwire

À ce stade, Tripwire est installé et configuré. Il est maintenant temps de vérifier si Tripwire fonctionne.

a) Créer les fichiers dans le système

sudo touch fil1 file2 file3 file4 file5

b) Exécuter le Tripwire pour vérifier si il détecte ou non les fichiers

sudo tripwire --check --interactive

Le résultat suivant, doit s'afficher

Open Source Tripwire(R) 2.4.3.7 Integrity Check Report

Report generated by:rootReport created on:Sun 05 Mar 2023 20:04:57 GMTDatabase last updated on:Never						
Report Summary:						
Host name:	Host name: raspberrypi					
Host IP address:	Host IP address: 127.0.1.1					
lost ID: None						
Policy file used:	Policy file used: /etc/tripwire/tw.pol					
Configuration file used:	guration file used: /etc/tripwire/tw.cfg					
Database file used:	Vatabase file used: /var/lib/tripwire/raspberrypi.twd					
command line used: tripwirecheckinteractive						
Rule Summary:						
Section: Unix File System						
Rule Name	Severity Level	Added	Removed	Modified		
Invariant Directories	66	0	0	0		

* Tripwire Data Files	100	1	0	0		
Other binaries	66	0	0	0		
Tripwire Binaries	100	0	0	0		
Other libraries	66	0	0	0		
Root file-system executables	100	0	0	0		
System boot changes	100	0	0	0		
Root file-system libraries (/lib)	100	0	0	0		
Critical system boot files	100	0	0	0		
* Other configuration files	66	5	0	1		
(/etc)						
Boot Scripts	100	0	0	0		
Security Control	66	0	0	0		
Root config files	100	0	0	0		
* Devices & Kernel information	100	8105	8115	0		
Total objects scanned: 151503						
Total violations found: 16227						
Object Summary:						
# Section: Unix File System						

f) Vérifier le rapport généré

twprint --print-report --twrfile /var/lib/tripwire/report/raspberrypi-20230305-194905.twr

8. Automatisation du rapport Tripwire

On peut configurer une tâche cron pour exécuter un Tripwire à un moment précis

a) Exécuter la tâche cron

sudo crontab -e

b) Sélectionner une option

Select an editor. To change later, run 'select-editor'.

1. /bin/nano <---- easiest

2. /usr/bin/vim.tiny

3. /bin/ed

c) Ajouter la ligne suivante et enregistrer le fichier

```
00 08 * * * /usr/sbin/tripwire --check
```

9. Consultation du rapport

Le fichier ci-dessus exécutera un Tripwire tous les matins à 08h00. On peut vérifier le rapport généré sur le dossier /var/lib/tripwire/report/

10. Commandes RaspberryPi

a) Liste des commandes basique à la gestion du serveur RaspberryPi

shutdown -h now # éteint le serveur en toute sécurité # shutdown -r now # redémarre le serveur en toute sécurité # apt install xrdp # installe le bureau à distance RDP # systemctl enable xrdp # active xrdp en tant que service système # apt install openssh-server # installe le SSH # systemctl enable sshd.service # active le service SSH au démarrage ###### Désactive la mise en veille ##### # systemctl mask sleep.target suspend.target hibernate.target hybrid-sleep.target

11. Conclusion

Tripwire IDS est installé et configuré avec succès sur le serveur **RaspberryPi Debian**. On peut désormais dormir tranquille.

Destiné au RaspberryPi (Raspbian), **Tripwire** fonctionne aussi parfaitement sur une distribution Debian, Fedora ou une Ubuntu en mode VPS ou sur un ordinateur personnel.

Debian 11 : https://howtoforge.com/how-to-install-and-configure-tripwire-ids-on-debian-10