

TP4-1 INTÉGRITÉ DES DONNÉES AVEC TRIPWIRE

Objectifs

Manipuler l'outil Tripwire qui permet de gérer une base de données de signatures de fichiers afin de vérifier si ceux-ci n'ont pas été corrompus.

Scénario

TripWire est un outil puissant et gratuit dont la fonction spécifique est la détection d'intrusion (IDS). Il met constamment à jour les fichiers système critiques et les rapports de contrôle au cas où ils auraient été modifiés ou supprimés par un pirate informatique ou un intrus.

TripWire enverra un message à l'administrateur système en cas de défaillance du système. TripWire est un outil à code source ouvert qui permettra au secteur informatique d'être averti en cas de modification du système Linux.

Ressources requises

- Machine virtuelle Ubuntu avec connexion Internet.

Faites des captures d'écran de toutes les commandes et les coller dans un fichier de réponses que vous devez déposer sur Teams

Étape 1 : Ouvrir une fenêtre de terminal dans Ubuntu.

- a. Connectez-vous à Ubuntu à l'aide des informations d'identification suivantes :
- b. Cliquez sur l'icône du terminal pour ouvrir une fenêtre de terminal.

Étape 2 : Mettre à jour le système

- a. Connecter vous en tant que root.
- b. Vous allez d'abord entrer cette commande pour mettre à jour tous les packages disponibles dans le système.

```
root@Ubuntu:~# apt install aptitude
```

```
root@Ubuntu:~# aptitude update
```

Étape 3 : Installer Tripwire

- c. Une fois le système mis à jour, taper la commande suivante pour le téléchargement et l'installation de TripWire:

```
root@Ubuntu:~# aptitude install tripwire
```

Lors de l'installation, on vous demande de spécifier deux phrase secrètes pour créer deux clés :

- Clé du site sera utilisée pour sécuriser le fichier de configuration twcfg.txt et le fichier de polices twpol.txt
- Clé locale sera utilisée pour sécuriser la base de données de Tripware

Les différents fichiers installés se situent dans les répertoires suivants :

- Fichiers de configuration /etc/tripwire/
- Binaires de tripwire /usr/sbin/
- Base de référence /var/lib/tripwire/
- Rapport générés : /var/lib/tripwire/report
- Documentation /usr/share/doc/tripwire/README.Debian

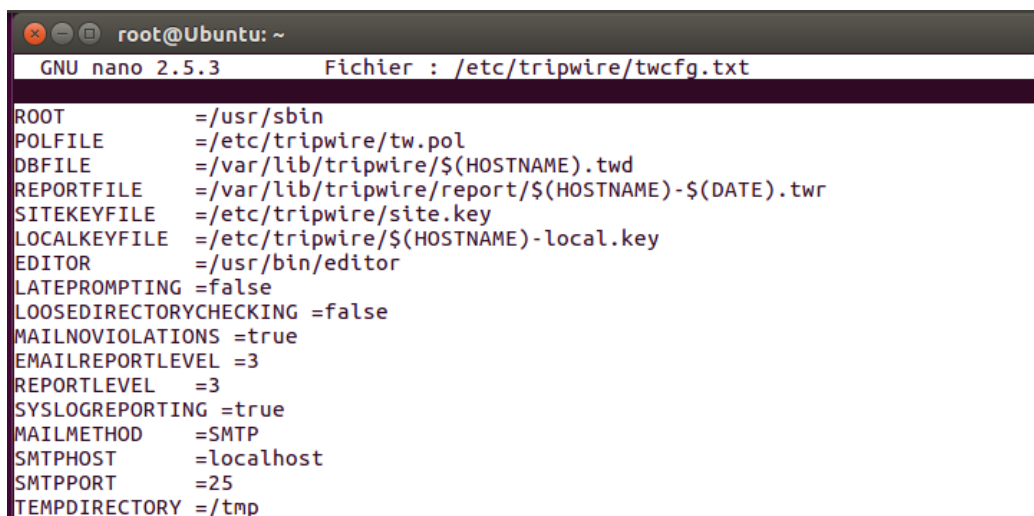
Pour solliciter l'aide en ligne du logiciel : `tripwire --help`

Fichier	Emplacement	Fonctionnalité
tripwire	/usr/sbin/	Permet de créer la base de référence, de vérifier l'intégrité du système, mettre à jour la base de référence
twadmin	/usr/sbin/	Permet de créer les clés (du site et local) Permet de créer les fichiers tw.pol et tw.cfg à partir de leur version en clair. Permet de signer des fichiers.
twprint	/usr/sbin/	Permet de générer le rapport ou la base en texte clair.
twcfg.txt	/etc/tripwire	Fichier de configuration tripwire. Il se transforme une fois crypté en tw.cfg.
twpol.txt	/etc/tripwire	Fichier de règles de police à appliquer. Celui qu'il faut adapter avec le plus de soin. Il se transforme en tw.pol une fois crypté

Étape 4: Éditer les fichiers tripwire

a. Éditer le fichiers de configuration twcfg.txt :

```
root@Ubuntu:~#gedit /etc/tripwire/twcfg.txt
```



```
root@Ubuntu: ~
GNU nano 2.5.3      Fichier : /etc/tripwire/twcfg.txt
ROOT                =/usr/sbin
POLFILE             =/etc/tripwire/tw.pol
DBFILE              =/var/lib/tripwire/$(HOSTNAME).twd
REPORTFILE          =/var/lib/tripwire/report/$(HOSTNAME)-$(DATE).twr
SITEKEYFILE         =/etc/tripwire/site.key
LOCALKEYFILE        =/etc/tripwire/$(HOSTNAME)-local.key
EDITOR              =/usr/bin/editor
LATEPROMPTING       =false
LOOSEDIRECTORYCHECKING =false
MAILNOVIOLATIONS    =true
EMAILREPORTLEVEL    =3
REPORTLEVEL         =3
SYSLOGREPORTING     =true
MAILMETHOD          =SMTP
SMTPHOST            =localhost
SMTPPORT           =25
TMPDIRECTORY        =/tmp
```

b. Éditer le fichier des règles twpol.txt

```
root@Ubuntu:~#gedit etc/tripwire/twpol.txt
```

```
root@Ubuntu: ~
GNU nano 2.5.3      Fichier : /etc/tripwire/twcfg.txt

ROOT           =/usr/sbin
POLFILE        =/etc/tripwire/tw.pol
DBFILE         =/var/lib/tripwire/${HOSTNAME}.twd
REPORTFILE     =/var/lib/tripwire/report/${HOSTNAME}-${DATE}.twr
SITEKEYFILE    =/etc/tripwire/site.key
LOCALKEYFILE   =/etc/tripwire/${HOSTNAME}-local.key
EDITOR         =/usr/bin/editor
LATEPROMPTING  =false
LOOSEDIRECTORYCHECKING =false
MAILNOVIOLATIONS =true
EMAILREPORTLEVEL =3
REPORTLEVEL    =3
SYSLOGREPORTING =true
MAILMETHOD     =SMTP
SMTPHOST       =localhost
SMTPPORT       =25
TMPDDIRECTORY  =/tmp
```

c. Ouvrir le dossier Tripwire : root@Ubuntu:~#ls -l /etc/tripwire/

```
root@Ubuntu:~# ls -l /etc/tripwire/
total 36
-rw-r--r-- 1 root root 931 sep 27 12:07 site.key
-rw-r--r-- 1 root root 4586 sep 27 12:07 tw.cfg
-rw-r--r-- 1 root root 510 mai 6 2015 twcfg.txt
-rw-r--r-- 1 root root 4159 sep 27 12:07 tw.pol
-rw-r--r-- 1 root root 6057 mai 6 2015 twpol.txt
-rw-r--r-- 1 root root 931 sep 27 12:07 Ubuntu-local.key
root@Ubuntu:~#
```

Étape 5 Générer la base de référence et faire une première vérification

a. Une fois l'outil TripWire installé, nous démarrons le service à l'aide de la commande suivante:

```
root@Ubuntu:~#tripwire -init
```

Et nous devons entrer le mot de passe local que nous avons créé précédemment.

```
root@Ubuntu:~# tripwire --init
Please enter your local passphrase:
Parsing policy file: /etc/tripwire/tw.pol
Generating the database...
*** Processing Unix File System ***
### Warning: File system error.
### Filename: /var/lib/tripwire/ubuntu.twd
### Aucun fichier ou dossier de ce type
### Continuing...
### Warning: File system error.
### Filename: /etc/rc.boot
### Aucun fichier ou dossier de ce type
### Continuing...
### Warning: File system error.
### Filename: /root/mail
### Aucun fichier ou dossier de ce type
### Continuing...
### Warning: File system error.
### Filename: /root/Mail
### Aucun fichier ou dossier de ce type
### Continuing...
### Warning: File system error.
### Filename: /root/.xsession-errors
### Aucun fichier ou dossier de ce type
### Continuing...
### Warning: File system error.
### Filename: /root/.xauth
### Aucun fichier ou dossier de ce type
### Continuing...
```

Le fichier de base de référence se trouve dans /var/lib/tripwire/Nom_serveur.twd
(Nom du serveur ici est « Ubuntu »)

b. Vérifier les fichiers

```
root@Ubuntu:~#tripwire -check
```

```

root@Ubuntu:~# tripwire --check
Parsing policy file: /etc/tripwire/tw.pol
*** Processing Unix File System ***
Performing integrity check...
### Warning: File system error.
### Filename: /etc/rc.boot
### Aucun fichier ou dossier de ce type
### Continuing...
### Warning: File system error.
### Filename: /root/mail
### Aucun fichier ou dossier de ce type
### Continuing...
### Warning: File system error.
### Filename: /root/Mail
### Aucun fichier ou dossier de ce type
### Continuing...
### Warning: File system error.
### Filename: /root/.xsession-errors
### Aucun fichier ou dossier de ce type
### Continuing...
### Warning: File system error.
### Filename: /root/.xauth
### Aucun fichier ou dossier de ce type
### Continuing...
### Warning: File system error.
### Filename: /root/.tcshrc
### Aucun fichier ou dossier de ce type
### Continuing...
### Warning: File system error.
### Filename: /root/.sawfish
### Aucun fichier ou dossier de ce type
### Continuing...

```

c. Afficher le fichier de rapport se trouve dans le dossier /var/lib/tripwire/report

```

root@Ubuntu:~# ls -l /var/lib/tripwire/
total 3332
drwxr-xr-x 2 root root    4096 sep 27 12:38 report
-rw-r--r-- 1 root root 3405636 sep 27 12:30 Ubuntu.twd

```

d. Lire le rapport

```

root@Ubuntu:~# twprint -m r --twrfile
/var/lib/tripwire/report/ubuntu-20200927-123703.twr

```

```

root@Ubuntu:~# twprint -m r --twrfile /var/lib/tripwire/report/ubuntu-20200927-1
23703.twr
Note: Report is not encrypted.
Open Source Tripwire(R) 2.4.2.2 Integrity Check Report

Report generated by:      root
Report created on:       dim 27 sep 2020 12:37:03 EDT
Database last updated on: Never

=====
Report Summary:
=====
Host name:                Ubuntu
Host IP address:          Unknown IP
Host ID:                  None
Policy file used:         /etc/tripwire/tw.pol
Configuration file used:  /etc/tripwire/tw.cfg
Database file used:       /var/lib/tripwire/ubuntu.twd
Command line used:        tripwire --check

=====
Rule Summary:
=====
Section: Unix File System
-----
Rule Name                  Severity Level   Added   Removed   Modified

```

e. Afficher le contenu de la base de référence :

```

root@Ubuntu:~# twprint -m d -print-dbfile |more

```

```
root@Ubuntu:~# twprint -m d --print-dbfile |more
Open Source Tripwire(R) 2.4.2.2 Database

Database generated by:      root
Database generated on:     din 27 sep 2020 12:28:26 EDT
Database last updated on:   Never

=====
Database Summary:
=====
Host name:                  Ubuntu
Host IP address:            Unknown IP
Host ID:                    None
Policy file used:           /etc/tripwire/tw.pol
Configuration file used:    /etc/tripwire/tw.cfg
Database file used:         /var/lib/tripwire/Ubuntu.twd
Command line used:          tripwire --init

=====
Object Summary:
=====

# Section: Unix File System
=====

Mode      UID      Size      Modify Time
-----

```

- f. Afficher les caractéristiques du fichier de configuration Tripwire

```
root@Ubuntu:~#twprint -m d -print-dbfile /etc/tripwire/tw.cfg
```

```
root@Ubuntu:~# twprint -m d --print-dbfile /etc/tripwire/tw.cfg
Object name: /etc/tripwire/tw.cfg

Property:      Value:
-----
Object Type    Regular File
Device Number  2049
Mode           -rw-r--r--
Num Links      1
UID            root (0)
GID            root (0)
Size           4586
Modify Time    din 27 sep 2020 12:07:33 EDT
Blocks         16
CRC32          A5PhfL
MD5            ARuk05BxBplx5HXNWokqh2
```

Étape 6: Créer et modifier un nouveau fichier

- Créer un dossier /test-tripwire
- Créer un fichier nommé file-test.txt dans /test-tripwire

Étape 7: Modifier la politique

Il faut maintenant modifier le fichier source de la politique /etc/tripwire/twpol.txt pour qu'il détecte toutes les modifications faites à ce fichier (fichier en lecture seul).

- Ajouter la règle de test vers la fin du fichier /etc/tripwire/twpol.txt

```
twpol.txt
/etc/tripwire

# rule file file-test.txt
#
(
    rulename = "rule file-test.txt",
    severity = $(SIG_MED)
)
{
    /test-tripwire/file-test.txt -> $(SEC_CRIT) ;
}

#
# Other configuration files
#
```

- b. Ensuite, créer un nouveau fichier de politique

```
root@Ubuntu:~# twadmin --create-polfile -S /etc/tripwire/site.key /etc/tripwire/twpol.txt
Please enter your site passphrase:
Wrote policy file: /etc/tripwire/tw.pol
root@Ubuntu:~#
```

Nous voyons que la politique de fichier a été écrite correctement.

- g. Une fois ces paramètres configurés, nous devons utiliser cette commande à nouveau pour que les modifications soient apportées.:

```
root@Ubuntu:~# tripwire --init
Please enter your local passphrase:
Parsing policy file: /etc/tripwire/tw.pol
Generating the database...
*** Processing Unix File System ***
```

Étape 8: Modifier le fichier et vérifier l'intégrité

- a. Modifier le fichier /test-tripwire/file-test.txt
b. Lancer une vérification et vous remarquerez la présence d'avertissement car ce fichier était contrôlé par Tripwire

```
root@Ubuntu:~# tripwire --check
Parsing policy file: /etc/tripwire/tw.pol
*** Processing Unix File System ***
Performing integrity check...
```

- c. Afficher le rapport généré et remarquer l'avertissement la modification du fichier test.

```
root@Ubuntu:~# twprint -m r --twrfile /var/lib/tripwire/report/Ubuntu-20200927-140122.twr |grep file-test.txt
* rule file-test.txt 66 0 0 1
  (/test-tripwire/file-test.txt)
Rule Name: rule file-test.txt (/test-tripwire/file-test.txt)
Modified object name: /test-tripwire/file-test.txt
root@Ubuntu:~#
```

- d. Mettre à jour la base de référence pour qu'elle accepte la modification du fichier test

```
root@Ubuntu:~# tripwire --update --twrfile /var/lib/tripwire/report/Ubuntu-20200927-140122.twr
Please enter your local passphrase:
Wrote database file: /var/lib/tripwire/Ubuntu.twd
root@Ubuntu:~#
```

Par défaut, tous les fichiers doivent être mis à jour dans la base de référence. Si on ne veut pas entériner certains changements, il faut retirer le «x» qui précède le chemin du fichier.

```
GNU nano 2.5.3 Fichier : /tmp/twtemptNa1ML
-----
Rule Name: rule file-test.txt (/test-tripwire/file-test.txt)
Severity Level: 66
-----
Remove the "x" from the adjacent box to prevent updating the database
with the new values for this object.

Modified:
[x] "/test-tripwire/file-test.txt"
=====
Object Detail:
=====
Section: Unix File System
-----
Rule Name: Tripwire Data Files (/var/lib/tripwire/Ubuntu.twd)
Severity Level: 100
-----
Added Objects: 1
-----
```

e. Lancer un nouveau check

```
root@Ubuntu:~# tripwire --check
Parsing policy file: /etc/tripwire/tw.pol
*** Processing Unix File System ***
Performing integrity check...
```

Un nouveau rapport sera créé (avec la date et l'heure), vous pouvez alors supprimer les anciens rapports.

f. Vérifier s'il y a eu des alertes après la mise à jour de la base de données des alertes Tripwire. Le rapport suivant n'affiche aucune alerte

```
root@Ubuntu:~# twprint -m r --twrfile /var/lib/tripwire/report/Ubuntu-20200927-1
41858.twr |grep file-test.txt
rule file-test.txt 66 0 0 0
(/test-tripwire/file-test.txt)
root@Ubuntu:~#
```

Étape 9: vérifier les notifications de tripwire par mail

Voir le lien suivant :

<https://techdirectarchive.com/2022/03/24/how-to-install-and-configure-tripwire-on-ubuntu/>

pour les tests vous pouvez avoir des E-mail temporaire, voici le lien : <https://temp-mail.org/>

Étape 10 : déposer sur teams et remettre une copie papier avant de partir