

Internet Security

TRIPWIRE - ATTACCO

Autore

GIORGIO UMBERTO
GAMBINO

Matricola

X81000851



UNIVERSITÀ
degli STUDI
di CATANIA

Contents

1	Introduzione	2
1.1	Tripwire	2
1.2	Obiettivo del progetto	2
2	Installazione e Configurazione di Tripwire	3
2.1	Apertura terminale	4
2.2	Passphrase per la prima della coppia di chiavi	4
2.3	Creazione site key passphrase	5
2.4	Passphrase per la seconda della coppia di chiavi	5
2.5	Creazione local key passphrase	6
2.6	Twcfg	6
2.7	Twpol	7
2.8	Inserisci site key	7
2.9	Valida site key	8
2.10	Inserisci local key	8
2.11	Valida local key	9
2.12	Tripwire installato	9
3	Comandi	10
4	Policy	12
4.1	Esempi di policy	13
5	Attacco	14
5.1	Analisi	14
5.2	Negazione del servizio	15
6	Conclusioni	17

1 Introduzione

1.1 Tripwire

Tripwire[1] è un IDS¹, flessibile e facile da usare. Il suo compito è quello di creare un punto di partenza (o baseline) del filesystem in modo da poter controllare grazie a delle policy, lo stato (modifiche del contenuto, nella data di modifica, nei permessi, negli attributi o di eventuali cancellazioni) dei file.

Se trova modifiche non autorizzate tra lo stato attuale e quello salvato, riporterà tutto all'amministratore, attraverso un rapporto e/o se configurato attraverso posta elettronica.

Sono presenti due versioni di Tripwire, una commerciale ed una Open source[2], entrambe le versioni del tool usano diversi algoritmi per testare l'integrità dei file, algoritmi che dovrebbero garantire un'elevata affidabilità.

1.2 Obiettivo del progetto

Andremo a configurare la versione Opensource di Tripwire su una macchina virtuale, cercheremo di trovare dei possibili attacchi.

In particolare vedremo se è possibile installare software o modificare file su una macchina dove vi è installato un IDS, senza che esso si accorga delle modifiche e quindi che l'amministratore della macchina non venga a conoscenza che c'è stata un'intrusione.

¹L'Intrusion Detection System è uno strumento, software o hardware, impiegato per individuare accessi non autorizzati ai computer oppure alle reti locali.

2 Installazione e Configurazione di Tripwire

L'installazione di Tripwire verrà effettuata su VirtualBox², come sistema operativo utilizzeremo una versione di Ubuntu, la 16.04.1 LTS.

Abbiamo due modi per effettuare l'installazione di Tripwire:

1. Clonazione del repository attraverso Github
2. RPM Package

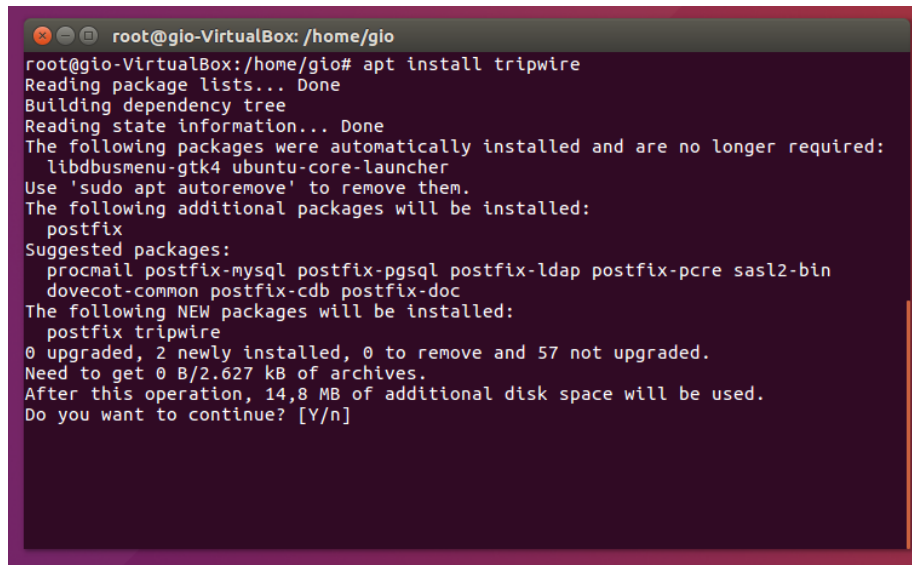
Se si vuole effettuare la prima, basta seguire i passi che si trovano nel README.md della repository stessa.

Noi andremo ad installare Tripwire nel secondo modo, che ci offre una piccola interfaccia per la generazione e il settaggio delle chiavi.

²E' un software per la virtualizzazione di sistemi x86

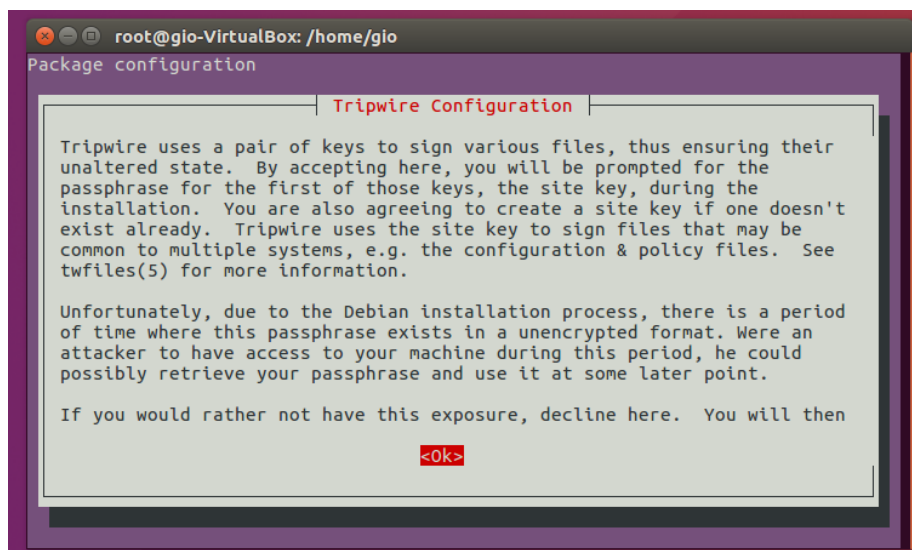
I passi da seguire per l'installazione sono i seguenti:

2.1 Apertura terminale



```
root@gio-VirtualBox: /home/gio
root@gio-VirtualBox:/home/gio# apt install tripwire
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libdbusmenu-gtk4 ubuntu-core-launcher
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  postfix
Suggested packages:
  procmail postfix-mysql postfix-pgsql postfix-ldap postfix-pcre sasl2-bin
  dovecot-common postfix-cdb postfix-doc
The following NEW packages will be installed:
  postfix tripwire
0 upgraded, 2 newly installed, 0 to remove and 57 not upgraded.
Need to get 0 B/2.627 kB of archives.
After this operation, 14,8 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

2.2 Passphrase per la prima della coppia di chiavi



```
root@gio-VirtualBox: /home/gio
Package configuration

Tripwire Configuration

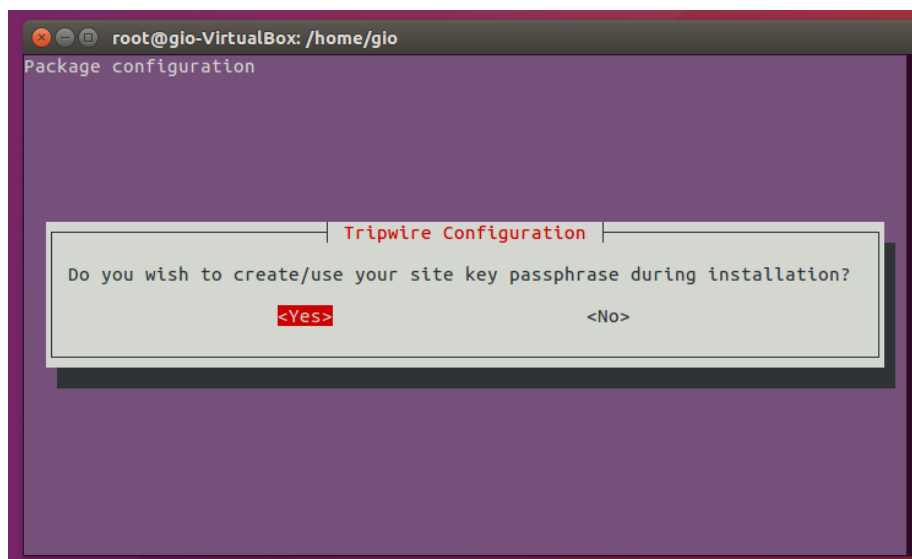
Tripwire uses a pair of keys to sign various files, thus ensuring their
unaltered state. By accepting here, you will be prompted for the
passphrase for the first of those keys, the site key, during the
installation. You are also agreeing to create a site key if one doesn't
exist already. Tripwire uses 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.

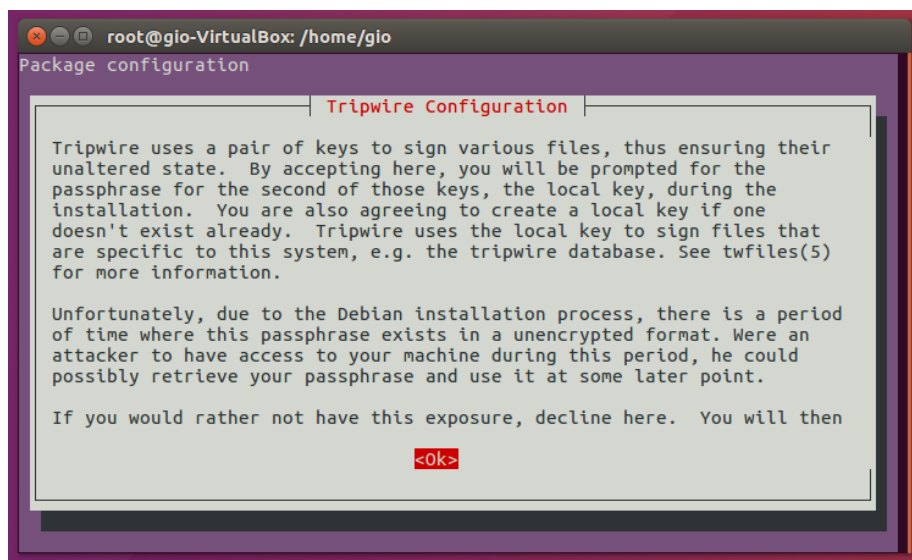
If you would rather not have this exposure, decline here. You will then

<Ok>
```

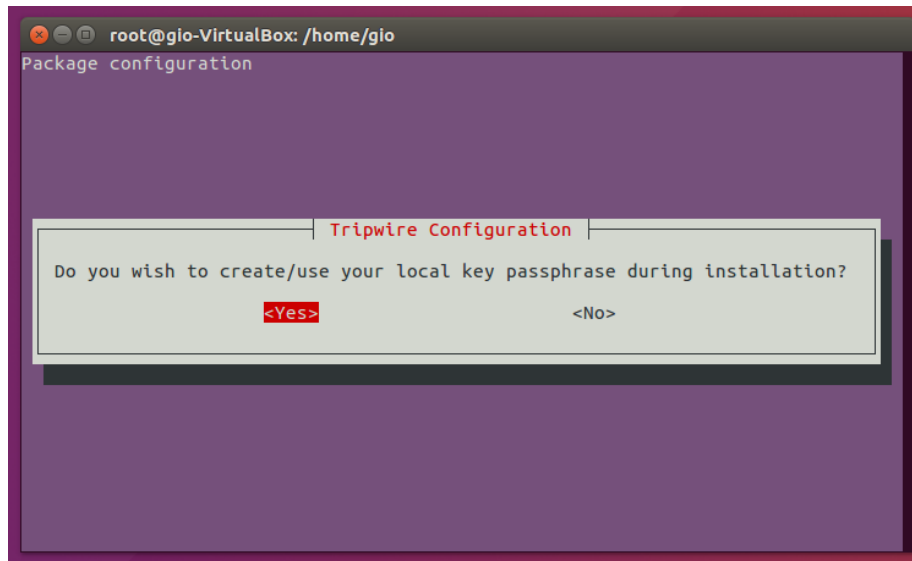
2.3 Creazione site key passphrase



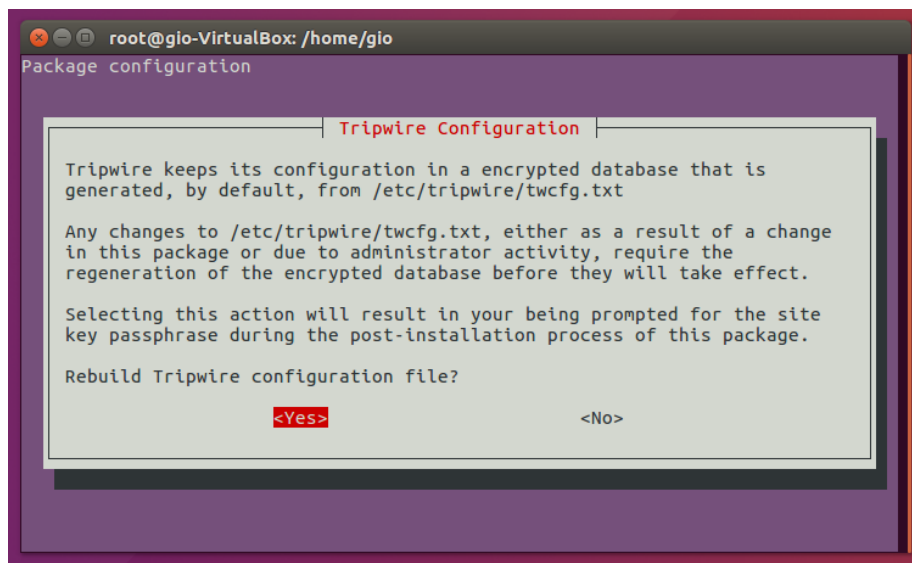
2.4 Passphrase per la seconda della coppia di chiavi



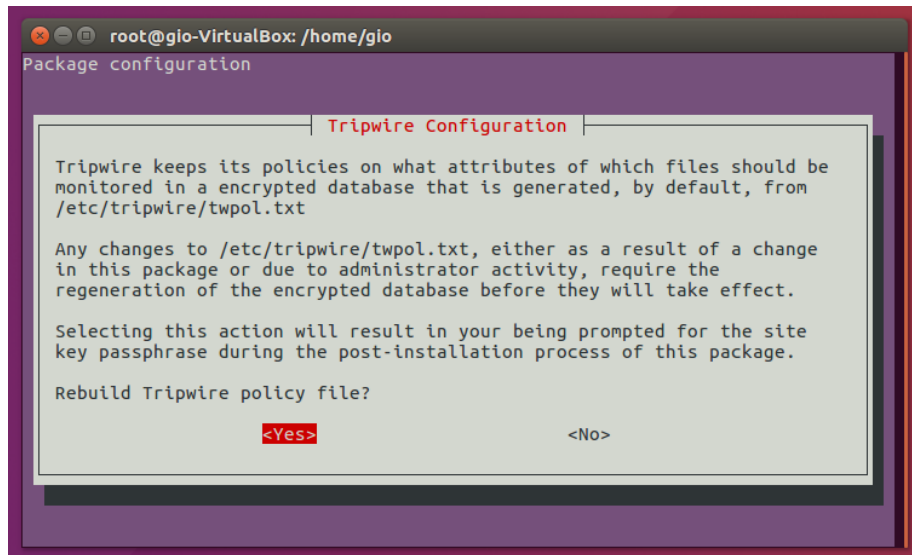
2.5 Creazione local key passphrase



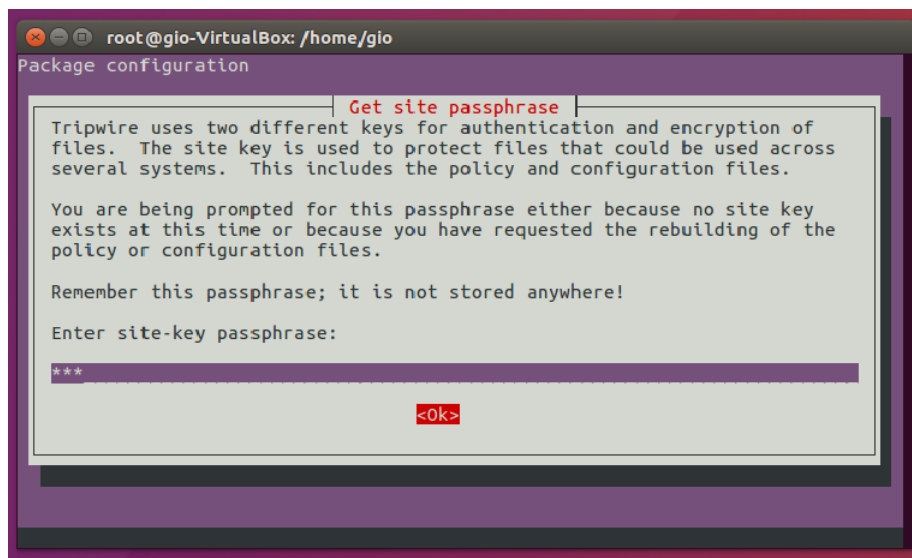
2.6 Twcfg



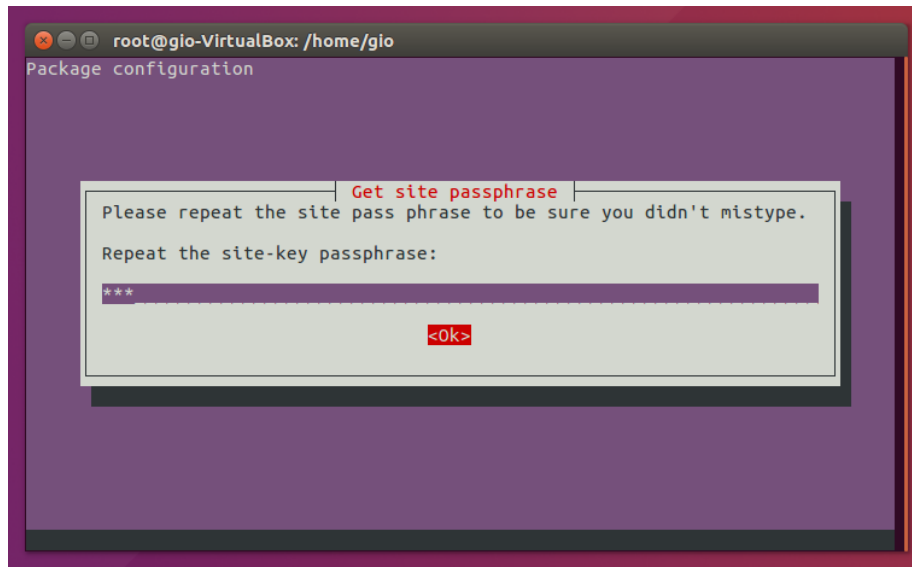
2.7 Twpol



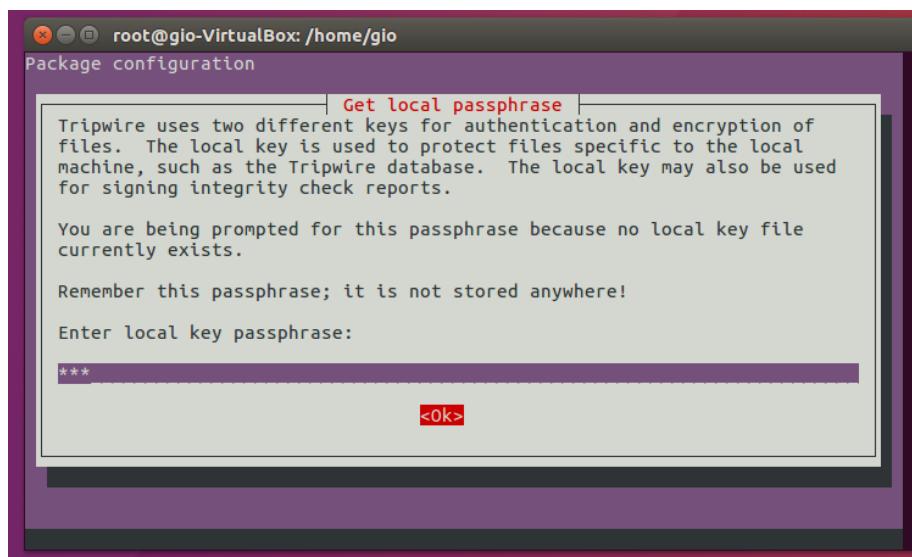
2.8 Inserisci site key



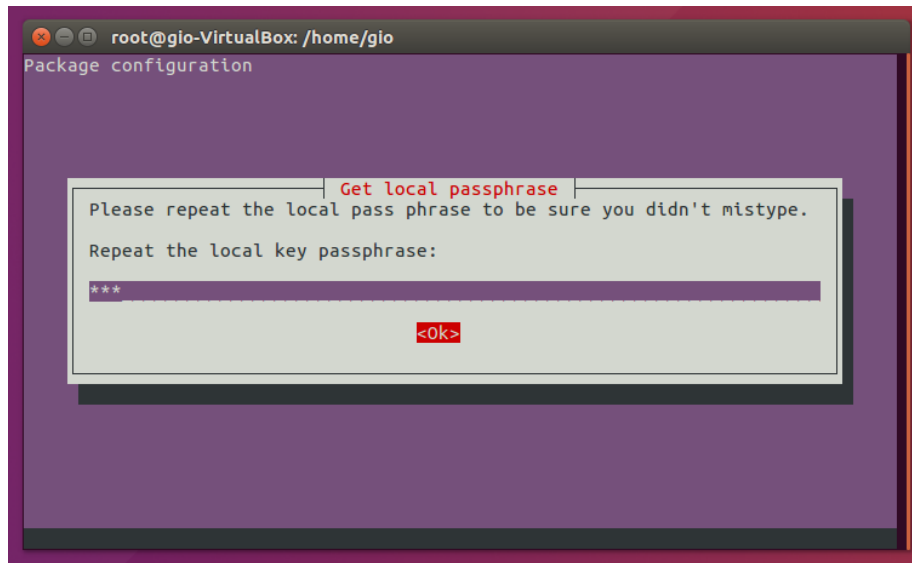
2.9 Valida site key



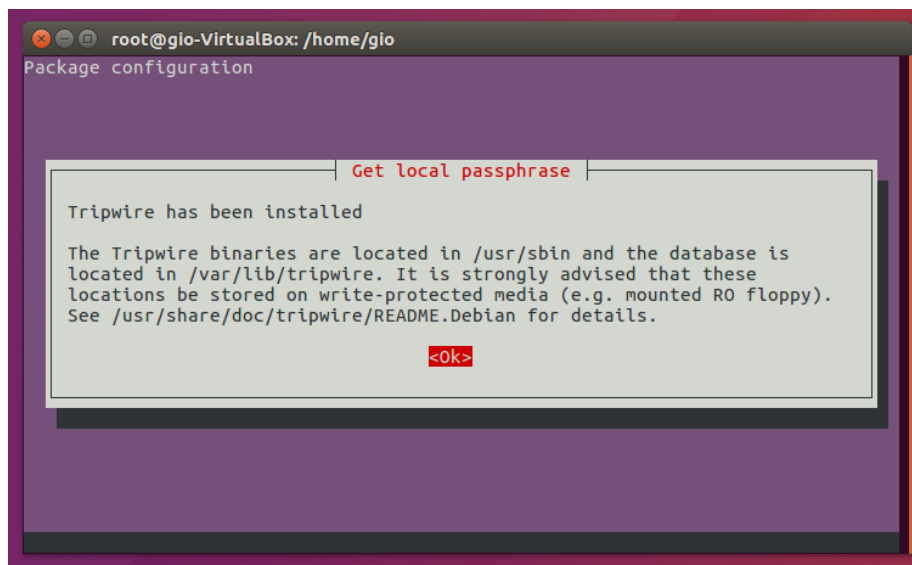
2.10 Inserisci local key



2.11 Valida local key



2.12 Tripwire installato



Dopo aver generato le chiavi, essendo la prima volta che installiamo Tripwire sulla macchina, bisognerà inizializzare il database, basandosi sulle regole contenute nel file di policy.

3 Comandi

Per inizializzare il database:

```
1      tripwire --init
```

Successivamente ti verrà richiesto di inserire la local key, essa viene utilizzata per proteggere il database e i report.

Per verificare se ci sono delle anomalie nel sistema, ti basta eseguire il seguente comando:

```
1      tripwire --check
```

Ti permette di confrontare il database con gli oggetti residenti nel filesystem, creando un report contenente le violazioni alle regole specificate nel file di policy.

Digitando invece:

```
1      tripwire --help
```

E' possibile vedere i restanti comandi (per aggiornare il database, modificare le policy e testare l'email qualora si volesse ricevere i report anche per via email).

Per visualizzare il file di configurazione:

```
1      twadmin --print-cfgfile
```

In questo modo è possibile vedere dove risiedono il file delle policy, il database, i report, le chiavi etc.

Solitamente i file di Tripwire sono collocati nel seguente modo:

- I programmi tripwire, twadmin e twprint si trovano in *usr/sbin/*
- Le chiavi (file *.key), file di configurazione (tw.cfg), policy (tw.pol) e script di inizializzazione (twinstall.sh) in *etc/tripwire*
- Il database (*.twd) in */var/lib/tripwire*
- I report (host-data report-ora report.twr) in */var/lib/tripwire/report*

Per visualizzare i report o il database:

```
1      twprint --print -report [options] [object1]
2      twprint --print -dbfile [options] [object1]
```

Per vedere gli options basta digitare:

```
1      twprint --help all
```

Per poter cambiare le policy basta aggiornare il file twpol.txt ed eseguire il seguente comando:

```
1      tripwire --update-policy
```

Dopo ti verrà richiesto di inserire la local key e la site key, non a caso, la modifica delle policy comporta la necessità di re-inizializzare di nuovo il database.

4 Policy

Per scrivere correttamente un file di policy dobbiamo seguire una sintassi ben precisa.

nome dell'oggetto -> proprietà della maschera

Per nome dell'oggetto si intende il path della directory o del file presente in una directory, mentre per proprietà della maschera intendiamo quale proprietà dell'oggetto esaminare o ignorare.

Una tabella che elenca le proprietà della maschera in Linux:

Proprietà	Significato
-	Ignora le seguenti proprietà
+	Controlla le seguenti proprietà
p	Permessi del file
i	Numero dell'inode
n	Numero di link
u	ID dell'utente proprietario
g	ID del gruppo proprietario
t	Tipo di file
s	Dimensione del file
d	Numero del device su cui è memorizzato l'inode associato al file
r	Numero del device puntato dall'inode
b	Numero di blocchi allocati
m	Timestamp di modifica
c	Timestamp di creazione/modifica dell'inode
l	Crescita del file in dimensione
a	Timestamp di accesso
C	Funzione di controllo CRC-32
M	Funzione hash MD5
S	Funzione SHA
H	Funzione hash HAVAL

4.1 Esempi di policy

Mostriamo alcuni esempi:

Definiamo che l'intera directory */bin* deve essere accessibile in sola lettura.

```
/bin -> +pinugsmdbfCMAG;
```

Potremmo anche scriverlo utilizzando delle macro già presenti, *Readonly* è l'alias di una maschera definita nel file di policy.

```
/bin -> $(Readonly);
```

Utilizzeremo gli stop points, specificando gli oggetti che non devono essere scanditi.

```
! nome dell'oggetto;
```

Vogliamo che nella directory */etc* non avvenga il controllo di due particolari file.

```
/etc -> $(ReadOnly);  
! /etc/file1;  
! /etc/file2;
```

E' presente un file **policyguide.txt** dove vi sono definite tutte le regole, con alcuni esempi per costruire le policy.

5 Attacco

5.1 Analisi

Come già accennato, vogliamo attaccare una macchina, dove vi è installato Tripwire. Per poter attaccare, dobbiamo tenere in considerazione molti fattori.

L'attacco è un processo continuo, che richiede uno scanning dell'ambiente. Dobbiamo cercare di ottenere più informazioni possibili sull'ambiente che ci circonda, vedere che mezzi abbiamo in nostro possesso e come sfruttarli. L'attacco chiaramente è limitato anche in base alle capacità e alle conseguenze che è disposto ad accettare l'attaccante.

La prima domanda che bisogna porsi è perché stiamo attaccando? L'amministratore della macchina ogni quanto esegue un check? Ha impostato qualche routine? Ci interessa non lasciare tracce? Cosa vogliamo ottenere? Abbiamo la possibilità di accedere fisicamente alla macchina? Ci sono CVE o Exploit su internet?

Possiamo immaginare uno scenario in cui l'attaccante, abbia accesso fisico alla macchina e voglia aggiungere/rimuovere/modificare file senza che Tripwire se ne accorga. L'intento è negare il servizio che offre Tripwire, e far credere all'admin che il problema sia dovuto ad un errore del disco.

5.2 Negazione del servizio

In che modo potremmo negare il servizio di Tripwire? Bisognerebbe negare la funzione del servizio `-check`. Per poter fare ciò dovremmo danneggiare il database, in modo che non possa verificare lo stato corrente con quello salvato. Eseguiamo il seguente codice sulla macchina per verificare se l'IDS è presente.

```
uname=`uname -n`  
twd=/var/lib/tripwire/$uname.twd  
  
if [ -d /etc/tripwire ]; then  
    echo "${WHI} ALERT: TRIPWIRE FOUND! ${RES}"  
  
    if [ -f /var/lib/tripwire/$uname.twd ]; then
```

Dopo aver avuto conferma che Tripwire è presente sulla macchina effettuiamo un semplicissimo comando.

```
chattr -isa $twd
```

Il comando `chattr` in Linux è un comando che viene utilizzato per modificare gli attributi di un file in una directory.

L'utilizzo principale di questo comando è quello di rendere diversi file non modificabili per utenti diversi dal superutente. Esiste la possibilità che un utente possa eliminare/modificare/leggere un file di cui non ne ha il diritto. Per evitare questo tipo di scenari, Linux fornisce "chattr".

Chattr in questo caso che attributi sta modificando?

1. Sta rimuovendo l'attributo `a`, rimuoverà il vincolo di aprire il file solo in modalità `append`.
2. Sta rimuovendo l'attributo `i`, rimuoverà il vincolo di essere immutabile.
3. Sta rimuovendo l'attributo `s`, rimuoverà il vincolo della `secure deletion`(se il file viene cancellato non verrà riempito di zeri).

Rimossi gli attributi, possiamo sovrascrivere il database, fornendo magari delle false informazioni all'amministratore.

```
echo "-----" > $twd
echo "Tripwire segment-faulted !" >> $twd
echo "-----" >> $twd
echo "" >> $twd
echo "The reasons for this may be: " >> $twd
echo "" >> $twd
echo "corrupted disc-geometry, possible bad disc-sectors" >> $twd
echo "corrupted files while checking for possible change etc." >> $twd
echo ""
echo "pls. rerun tripwire to build the database again!" >> $twd
echo "" >> $twd
```

Così facendo l'amministratore, crederà che ci sia stato un errore sul disco e dovrà inizializzare nuovamente il database.

Per poter sferrare questo attacco, abbiamo bisogno dei permessi di root. Ma aspetta se abbiamo bisogno dei permessi di root, perché vogliamo sovrascrivere il database di Tripwire e non rimuoverlo direttamente dalla macchina?

Con un pò di Ingegneria sociale³, cerchiamo di far credere all'amministratore che il problema sia nato da un problema della macchina e non che sia dovuto da un attaccante. Dobbiamo cercare di portare fuori pista l'amministratore, e cercare di lasciare meno tracce possibili.

Per ottenere i permessi di root potremmo fare una Privilege escalation⁴.

La versione di Ubuntu su cui stiamo operando soffre di una vulnerabilità al Kernel. Scarichiamo l'exploit[3] e lanciamolo sulla macchina, da questo momento in poi l'attaccante non dovrà fare altro che sovrascrivere il database, magari creando un file bash apposito e successivamente avrà il via libera per fare quello che vuole.

³E' una disciplina che sfrutta processi cognitivi di influenzamento, inganno e manipolazione per indurre una persona a compiere un'azione o a comunicare informazioni riservate.

⁴E' lo sfruttamento di una falla, di un errore di progetto o di configurazione di un software applicativo o di un sistema operativo al fine di acquisire il controllo di risorse di macchina normalmente precluse a un utente o a un'applicazione

6 Conclusioni

La tipologia di attacco che è stata mostrata ha delle limitazioni, funziona solamente se l'admin non ha delle copie di backup del database, anzichè inizializzare nuovamente il database fornendo una nuova baseline, potrebbe reinizializzare il database con una copia di backup. In questo modo potrà verificare se ci sono state delle intrusioni. Personalmente non avevo mai avuto modo fino ad'ora di installare un IDS su una macchina, ne tanto meno di provare ad attaccarlo, mi sono immedesimato nell'attaccante, ho cercato delle CVE relative alla versione Opensource, ma ho trovato ben poco e non sono riuscito ad exploitare. Il pezzo di codice che ho utilizzato per attaccare, è stato estratto dalla rootkit shv5[4] presente su GitHub.

Tripwire per garantire una maggiore sicurezza dovrebbe essere installato prima che la macchina venga esposta ad Internet o prima che qualcun'altro oltre il "proprietario" vi possa accedere. Tutto ciò che viene fatto prima dell'installazione di Tripwire verrà inclusa nel suo database, quindi chiunque potrebbe installare un keylogger o un software nocivo prima dell'installazione. In questo modo non otterremo sicurezza, cosa che dovrebbe essere garantita dall'IDS. L'utilizzo degli IDS è fondamentale, per monitorare ciò che accade all'interno della nostra macchina. Fornire utili informazioni su intrusioni avvenute, fare diagnosi e correzioni di eventuali debolezze. E' un ottimo strumento, che aggiunge uno strato di sicurezza in più.

References

- [1] Wikipedia contributors, “Open source tripwire — Wikipedia, the free encyclopedia.” https://en.wikipedia.org/w/index.php?title=Open_Source_Tripwire&oldid=993145595, 2020.
- [2] brc0x1, “Tripwire open source.” <https://github.com/Tripwire/tripwire-open-source>, 2019.
- [3] rlarabee, “Linux kernel < 4.13.9 (ubuntu 16.04 / fedora 27) - local privilege escalation.” <https://www.exploit-db.com/exploits/45010>, 2018.
- [4] CCrashBandicot, “Shv5 rootkit.” <https://github.com/CCrashBandicot/shv5>, 2015.