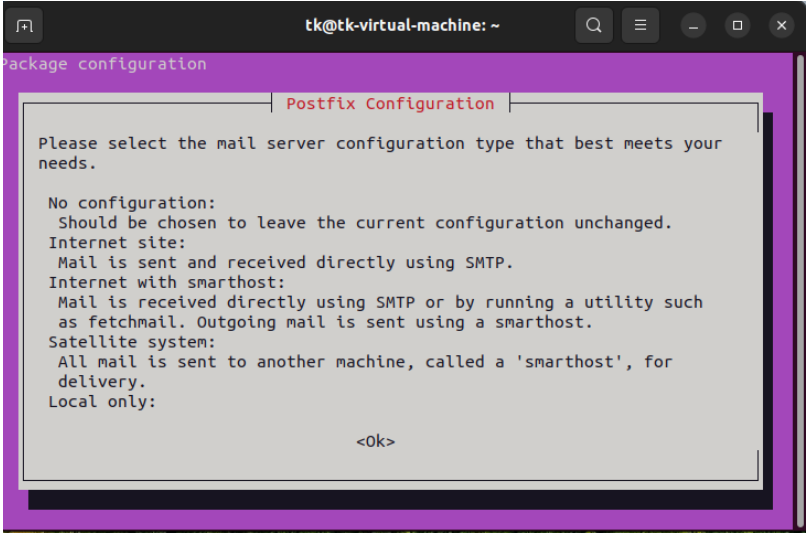
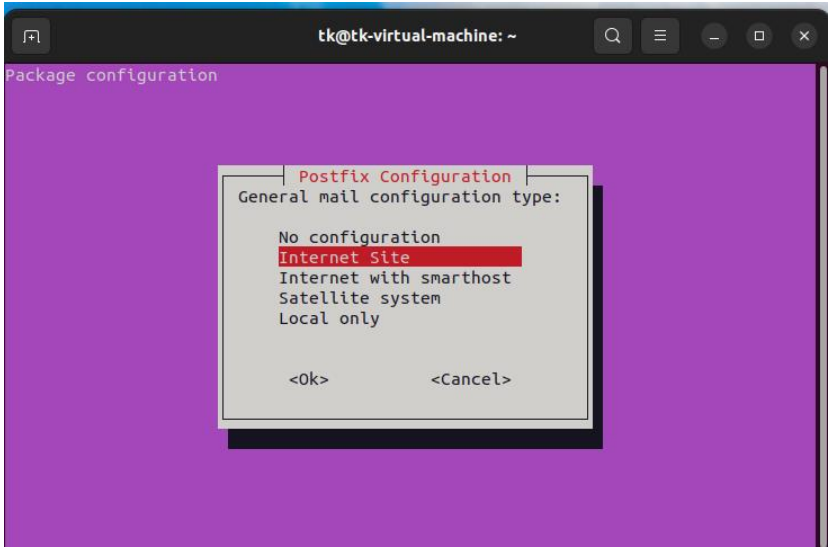


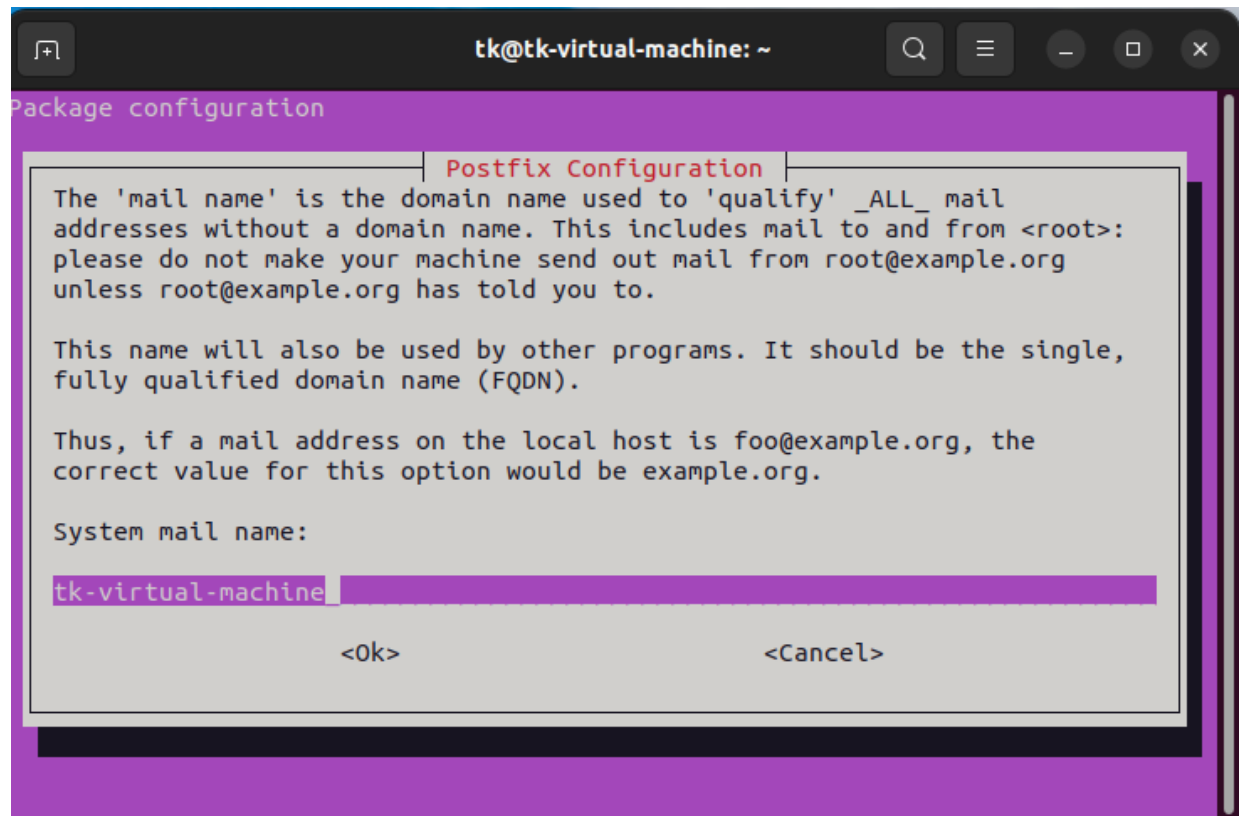
## Tripwire

Tripwire is a security auditing and intrusion detection tool. It works by scanning specific objects in a system and then comparing them to a reference database of known values. If any discrepancies are found, Tripwire will alert the user and a log file is generated. The tool is used to detect any changes that may have been made to critical system components, such as configuration files, system binaries, and libraries. It is also used to monitor user activity, such as login, file access, and other user-initiated actions.

### Install Tripwire on Ubuntu 22.04 LTS

Step 1	<p>Tripwire package for Ubuntu is available from the apt repository. Install it by running:</p> <pre>sudo apt update</pre> <pre>sudo apt install tripwire</pre>  <p>After running the second command after a while you will see a Posfix Configuration message where click &lt;Ok&gt;. To move to &lt;Ok&gt; button you can use Tab button from keyboard.</p>
Step 2	<p>After clicking &lt;Ok&gt; you will see like following</p>  <p>Click Internet Site or No configuration. Either choice is fine.</p>
Step 3	<p>Now in Postfix Configuration System mail name: you can keep as it is.</p>

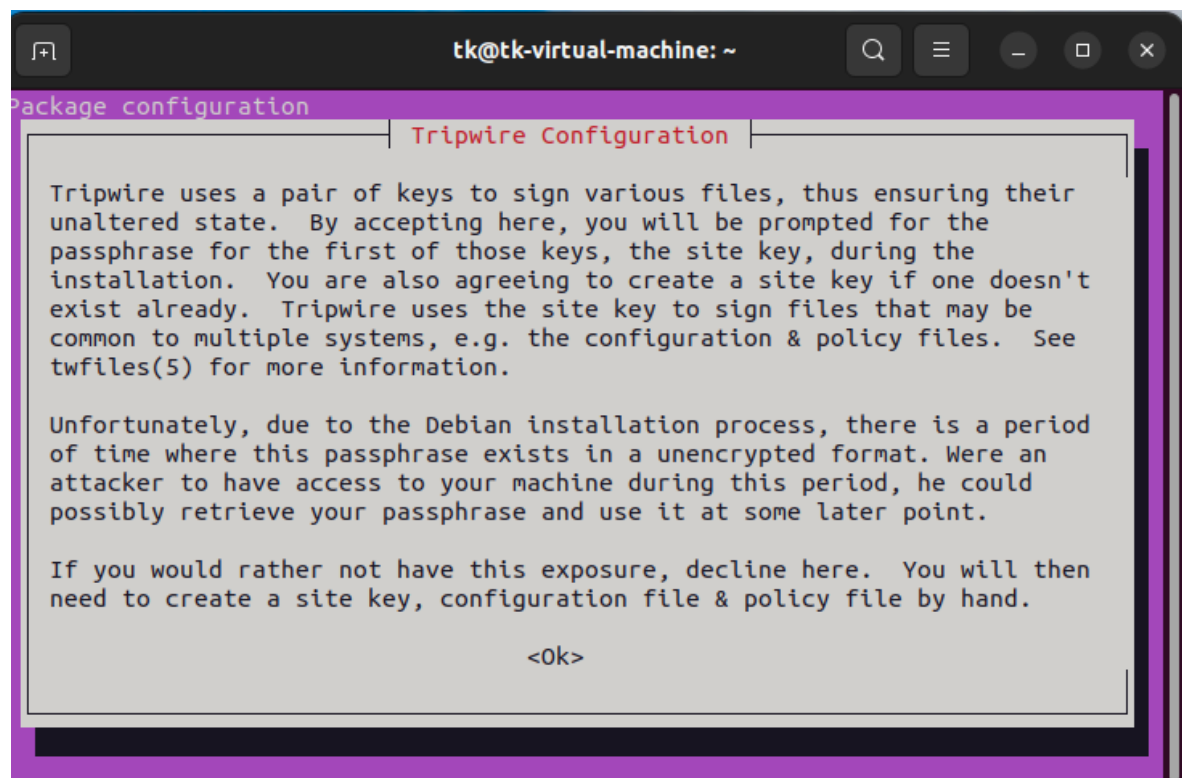
Please note down the 'System mail name', which you will need in later steps.



Just click <Ok>

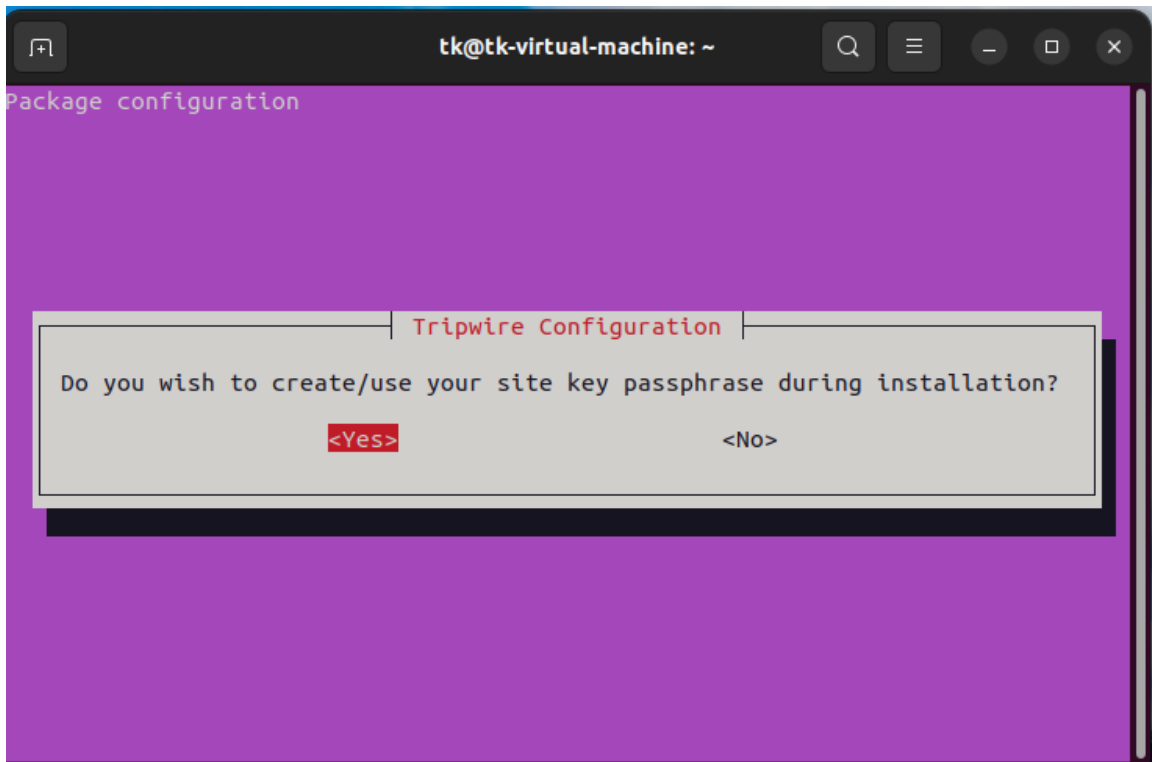
Step 4

Click <Ok> or <Yes> for Tripwire Configuration



Step 5

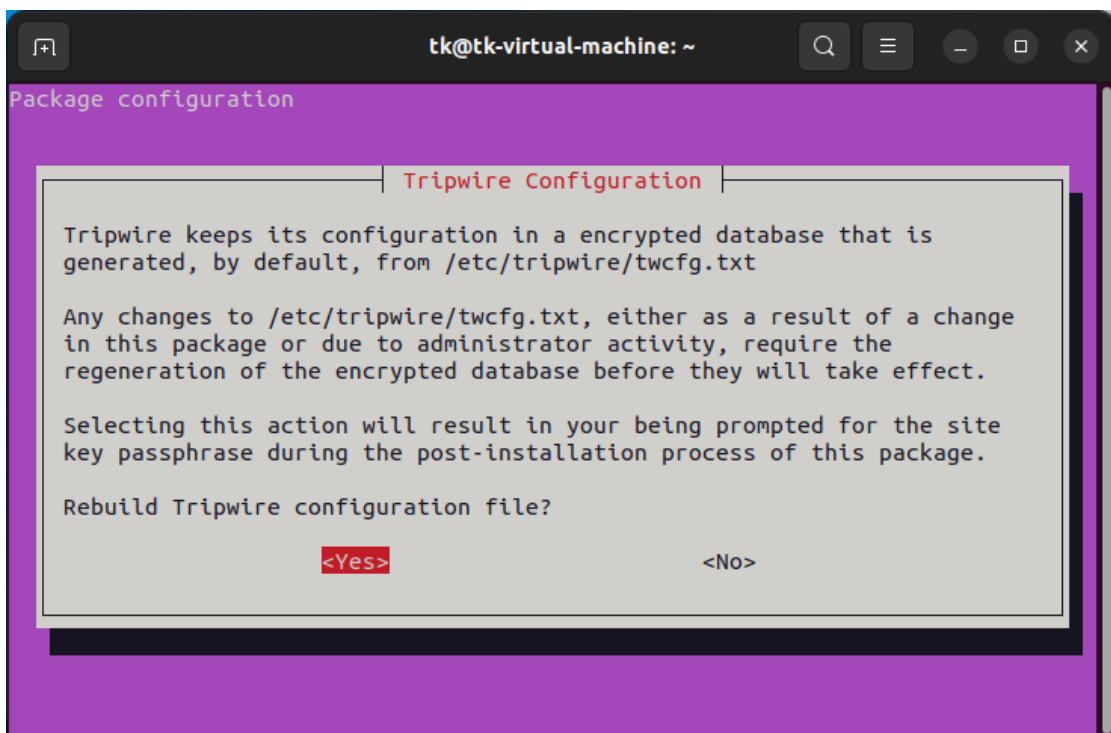
Tripwire uses two keys. One is the site key which is used to maintain administration of the config files and the other is the local key, which is used to maintain the database of hashes. The config files and database are normally encrypted, however, the starting configuration installed is not encrypted.



Now hit <Yes> and set your two passphrase. **Passphrase usually like a password. So, using an alphanumeric and with special character helps to set it at once. I used “phras3thi\$”**

Step 6

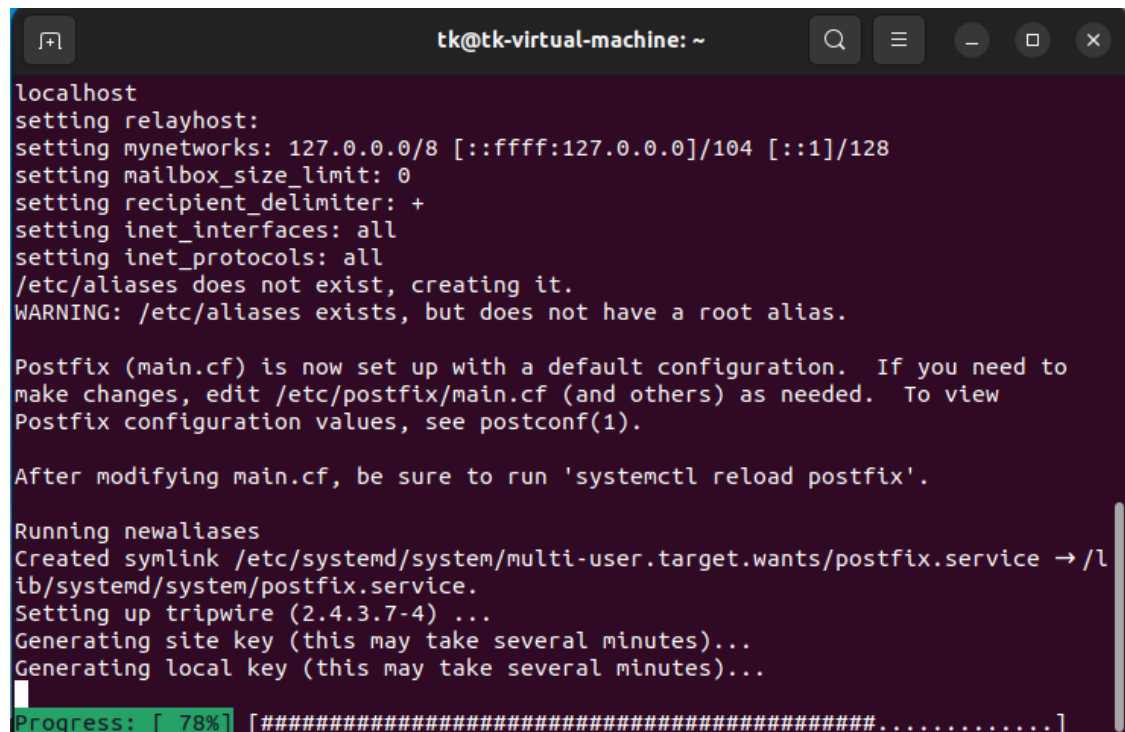
After setting two passphrase. You have to rebuild the Tripwire configuration.



Now hit <Yes>.

Step 7

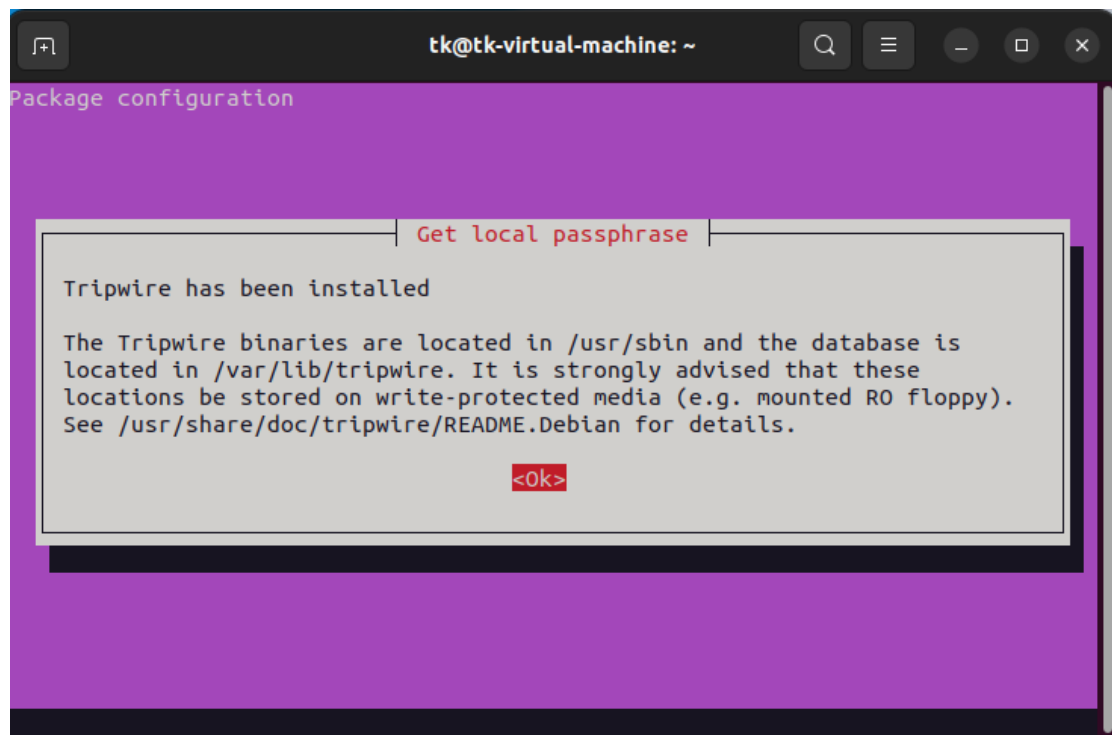
This installation is an interactive process, it will ask you a couple of questions. Answer then accordingly to install Tripwire on Ubuntu 22.04 LTS.




```
tk@tk-virtual-machine: ~  
localhost  
setting relayhost:  
setting mynetworks: 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128  
setting mailbox_size_limit: 0  
setting recipient_delimiter: +  
setting inet_interfaces: all  
setting inet_protocols: all  
/etc/aliases does not exist, creating it.  
WARNING: /etc/aliases exists, but does not have a root alias.  
  
Postfix (main.cf) is now set up with a default configuration. If you need to  
make changes, edit /etc/postfix/main.cf (and others) as needed. To view  
Postfix configuration values, see postconf(1).  
  
After modifying main.cf, be sure to run 'systemctl reload postfix'.  
  
Running newaliases  
Created symlink /etc/systemd/system/multi-user.target.wants/postfix.service → /l  
ib/systemd/system/postfix.service.  
Setting up tripwire (2.4.3.7-4) ...  
Generating site key (this may take several minutes)...  
Generating local key (this may take several minutes)...  
Progress: [ 78%] [#####.....]
```

Step 8

After successful installation of Tripwire you will see a message like this. Hit <Ok>



Step 9	<p>No go to /etc/tripwire directory</p> <pre>tk@tk-virtual-machine:~\$ cd /etc/tripwire/ tk@tk-virtual-machine:/etc/tripwire\$</pre> <p>With <b>cd /etc/tripwire</b> command</p>
Step 10	<p>Now do a long listing to see the file contains.</p> <pre>tk@tk-virtual-machine:/etc/tripwire\$ ls -l total 36 -rw----- 1 root root 931 Jan 4 14:44 site.key -rw----- 1 root root 931 Jan 4 14:44 tk-virtual-machine-local.key -rw-r--r-- 1 root root 4586 Jan 4 14:44 tw.cfg -rw-r--r-- 1 root root 510 Nov 10 2021 twcfg.txt -rw-r--r-- 1 root root 4159 Jan 4 14:44 tw.pol -rw-r--r-- 1 root root 6057 Nov 10 2021 twpol.txt tk@tk-virtual-machine:/etc/tripwire\$</pre> <p>Now that the installation has been successful, we need to initialize database so that tripwire can start its work.</p>
Step 11	<p>In twcfg.txt file, we will modify REPORTLEVEL to 4, which is the maximum number/level.</p> <p>sudo gedit twcfg.txt</p> <pre>tk@tk-virtual-machine:/etc/tripwire\$ sudo gedit twcfg.txt [sudo] password for tk:</pre>
Step 12	<p>After this file will open.</p>  <pre>1 ROOT      =/usr/sbin 2 POLFILE   =/etc/tripwire/tw.pol 3 DBFILE    =/var/lib/tripwire/\${HOSTNAME}.twd 4 REPORTFILE =/var/lib/tripwire/report/\${HOSTNAME}-\${DATE}.twr 5 SITEKEYFILE =/etc/tripwire/site.key 6 LOCALKEYFILE =/etc/tripwire/\${HOSTNAME}-local.key 7 EDITOR    =/usr/bin/editor 8 LATEPROMPTING =false 9 LOOSEDIRECTORYCHECKING =false 10 MAILNOVIOLATIONS =true 11 EMAILREPORTLEVEL =3 12 REPORTLEVEL =4 13 SYSLOGREPORTING =true 14 MAILMETHOD   =SMTP 15 SMTPHOST     =localhost 16 SMTPPORT     =25 17 TEMPDIRECTORY =/tmp</pre> <p>In the highlighted line set to 4. Usually, it stays in 3.</p> <p>Save the file and close the file.</p>
Step 13	<p>Generate a configuration file after the change:</p> <p>Use command: <b>sudo twadmin -m F -c tw.cfg -S site.key twcfg.txt</b></p> <pre>tk@tk-virtual-machine:/etc/tripwire\$ sudo twadmin -m F -c tw.cfg -S site.key twcfg.txt Please enter your site passphrase: Wrote configuration file: /etc/tripwire/tw.cfg tk@tk-virtual-machine:/etc/tripwire\$</pre> <p>Please use passphrase you did in Step 5, e.g., in this case it is “phras3thi\$”.</p>

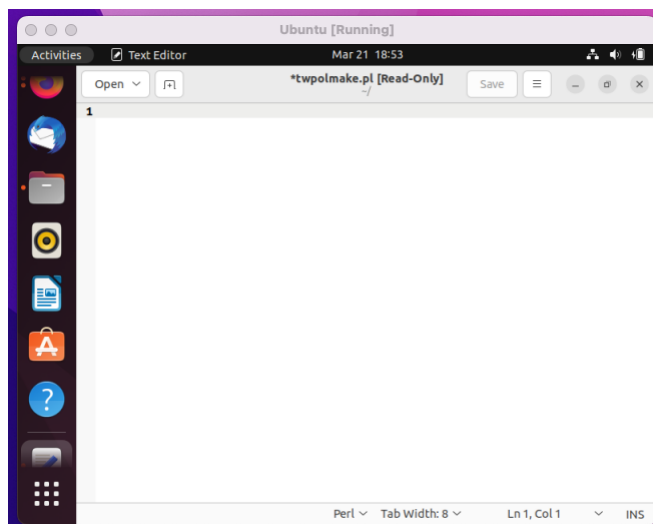
---

### Step 14

To optimize Tripwire Policy file, now create a file named twpolmake.pl in /etc/tripwire directory.

Command: **sudo gedit twpolmake.pl**

You will see blank file as below:



You will need to copy the following content from the link and paste it in the blank file

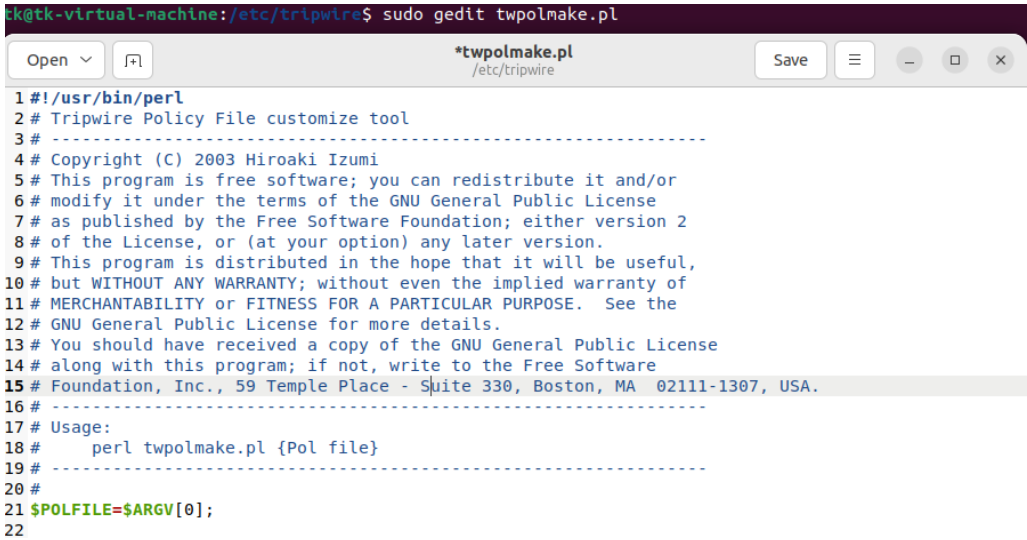

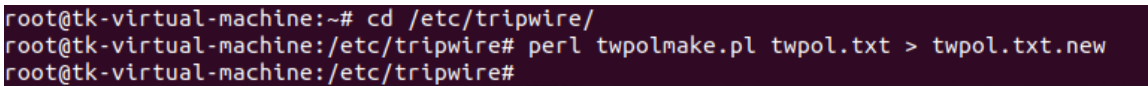
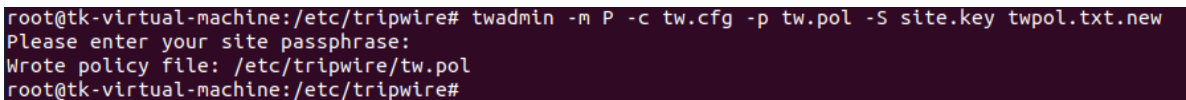
Link: <https://github.com/Tripwire/tripwire-open-source/blob/master/contrib/twpolmake.pl>

```
#!/usr/bin/perl
# Tripwire Policy File customize tool
# -----
# Copyright (C) 2003 Hiroaki Izumi
# This program is free software; you can redistribute it and/or
# modify it under the terms of the GNU General Public License
# as published by the Free Software Foundation; either version 2
# of the License, or (at your option) any later version.
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
# GNU General Public License for more details.
# You should have received a copy of the GNU General Public License
# along with this program; if not, write to the Free Software
# Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.
# -----
# Usage:
# perl twpolmake.pl {Pol file}
# -----
#
$POLFILE=$ARGV[0];

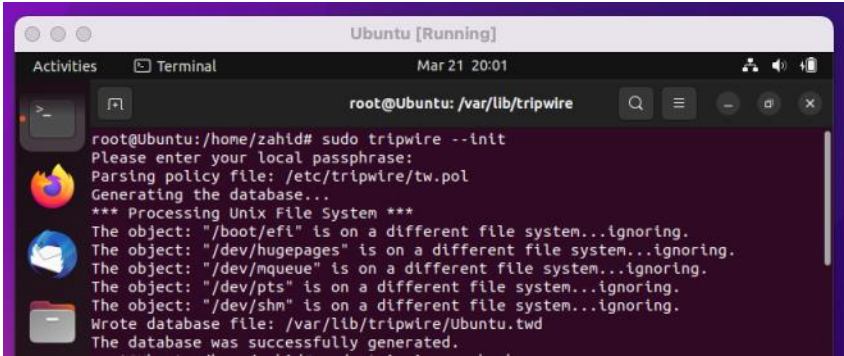
open(POL,"$POLFILE") or die "open error: $POLFILE" ;
my($myhost,$sthost) ;
my($ssharp,$stpath,$scond) ;
my($SINRULE) = 0 ;

while (<POL>) {
  chomp;
  if ((($sthost) =~ /^HOSTNAME\s*=\s*(.*)\s*;/) ) {
    $myhost = `hostname` ; chomp($myhost) ;
    if ($sthost ne $myhost) {
      $_="HOSTNAME=\"$myhost\";" ;
    }
  }
  elsif (/^{/ ) {
    $SINRULE=1 ;
  }
  elsif (/^/ ) {
    $SINRULE=0 ;
  }
  elsif ($SINRULE == 1 and ($ssharp,$stpath,$scond) =~ /^(\s*%\s*?)(\s*)(\s+>)(\s+,\s+)(\s+)$/) {
    $ret = ($ssharp =~ s/\s*//g) ;
    if ($stpath eq '/sbin/e2fsadm' ) {
      $scond =~ s/;/s+(tune2fs.*)$/; \##$/ ;
    }
    if (! -s $stpath) {
      $_ = "$ssharp#$stpath$scond" if ($ret == 0) ;
    }
    else {

```

	<pre>         \$_ = "\$sharp\$tpath\$cond" ;     } } print "\$_\n" ; } close(POL) ; </pre>  <p>Save and close the file.</p>
Step 15	<p>Now elevate to root privileges</p> 
Step 16	<p>Again, go to <b>/etc/tripwire/</b> directory</p> <pre>cd /etc/tripwire/</pre> <p>To create configuration run the following command</p> <pre>perl twpolmake.pl twpol.txt &gt; twpol.txt.new</pre> 
Step 17	<p>To write policy now run the following command.</p> <pre><b>twadmin -m P -c tw.cfg -p tw.pol -S site.key twpol.txt.new</b></pre> <p>Please use passphrase you did in Step 5, e.g., in this case it is “phras3thi\$”.</p> 
Step 18	<p>Now create tripwire database.</p> <pre><b>tripwire -m i -s -c tw.cfg</b></pre> <p>Please use passphrase you did in Step 5, e.g., in this case it is “phras3thi\$”.</p>



	<pre>root@tk-virtual-machine:/etc/tripwire# tripwire -m i -s -c tw.cfg Please enter your local passphrase: ### Warning: File system error. ### Filename: /var/lib/tripwire/tk-virtual-machine.twd ### No such file or directory ### Continuing... root@tk-virtual-machine:/etc/tripwire#</pre> <p><b>It will take some time, thus please wait.</b></p> <p>Warning can be ignored.</p>
Step 19	<p>Now after creating new database, we need to initialize the tripwire.</p> <pre>sudo tripwire --init</pre> 
Step 20	<p>To print the whole database:</p> <pre>twprint -m d -d /var/lib/tripwire/{your-machine-name}.twd</pre> <p><b>{your-machine-name}</b> should be replaced with the name you have given in Step 3.</p> <pre>root@tk-virtual-machine:/etc/tripwire# twprint -m d -d /var/lib/tripwire/tk-virtual-machine.twd</pre>
Step 21	<p>Test tripwire by executing checking manually</p> <pre>tripwire -m c -s -c /etc/tripwire/tw.cfg</pre> <pre>root@tk-virtual-machine:/etc/tripwire# tripwire -m c -s -c /etc/tripwire/tw.cfg</pre>
Step 22	<p>The -t argument specifies the level of report verbosity, where 0 is a single line summary of the report contents, and 4 displays all gathered attributes on all changed objects. The report level defaults to 3 if not specified on the command line or via the REPORTLEVEL config file option. Example:</p> <pre>twprint -m r -t 4 -r /var/lib/tripwire/report/{your-machine-name}.twr</pre>



	<pre>root@tk-virtual-machine:~# twprint -m r -t 4 -r /var/lib/tripwire/report/tk-virtual-machine-20230104-150740.twr Note: Report is not encrypted. Open Source Tripwire(R) 2.4.3.7 Integrity Check Report  Report generated by:      root Report created on:       Wed 04 Jan 2023 03:07:40 PM EST Database last updated on: Never  ===== Report Summary: =====  Host name:                tk-virtual-machine Host IP address:          127.0.1.1 Host ID:                  None Policy file used:         /etc/tripwire/tw.pol Configuration file used:  /etc/tripwire/tw.cfg Database file used:       /var/lib/tripwire/tk-virtual-machine.twd Command line used:        tripwire -m c -s -c /etc/tripwire/tw.cfg</pre>
	<p>End of a successful report.</p> <pre>Modified: "/etc/tripwire"  ===== Error Report: =====  No Errors  ----- *** 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. root@tk-virtual-machine:/etc/tripwire#</pre>
Step 23	