A

Seminar report

On

# Tripwire

Submitted in partial fulfillment of the requirement for the award of degree
Of CSE

**SUBMITTED TO:**

www.studymafia.org

**SUBMITTED BY:**

www.studymafia.org

# Acknowledgement

I would like to thank respected Mr…….. and Mr. ……..for giving me such a wonderful opportunity to expand my knowledge for my own branch and giving me guidelines to present a seminar report. It helped me a lot to realize of what we study for.

Secondly, I would like to thank my parents who patiently helped me as i went through my work and helped to modify and eliminate some of the irrelevant or un-necessary stuffs.

Thirdly, I would like to thank my friends who helped me to make my work more organized and well-stacked till the end.

Next, I would thank Microsoft for developing such a wonderful tool like MS Word. It helped my work a lot to remain error-free.

Last but clearly not the least, I would thank The Almighty for giving me strength to complete my report on time.

# Preface

I have made this report file on the topic **Tripwire**; I have tried my best to elucidate all the relevant detail to the topic to be included in the report. While in the beginning I have tried to give a general view about this topic.

My efforts and wholehearted co-corporation of each and everyone has ended on a successful note. I express my sincere gratitude to …………..who assisting me throughout the preparation of this topic. I thank him for providing me the reinforcement, confidence and most importantly the track for the topic whenever I needed it.

## Content

# INTRODUCTION

Tripwire is a reliable intrusion detection system. It is a software tool that checks to see what has changed in your system. It mainly monitors the key attribute of your files; by key attribute we mean the binary signature, size and other related data. Security and operational stability must go hand in hand; if the user does not have control over the various operations taking place, then naturally the security of the system is also compromised. Tripwire has a powerful feature which pinpoints the changes that has taken place, notifies the administrator of these changes, determines the nature of the changes and provide you with information you need for deciding how to manage the change.

Tripwire Integrity management solutions monitor changes to vital system and configuration files. Any changes that occur are compared to a snapshot of the established good baseline. The software detects the changes, notifies the staff and enables rapid recovery and remedy for changes. All Tripwire installation can be centrally managed. Tripwire software's cross platform functionality enables you to manage thousands of devices across your infrastructure.

Security not only means protecting your system against various attacks but also means taking quick and decisive actions when your system is attacked.

First of all we must find out whether our system is attacked or not, earlier system logs are certainly handy. You can see evidences of password guessing and other suspicious activities. Logs are ideal for tracing steps of the cracker as he tries to penetrate into the system. But who has the time and the patience to examine the logs on a daily basis??

# BASIC PURPOSE OF TRIPWIRE

Almost the same principle is used in computers. If any change is met upon while comparing the old values to the new ones, or if any data is being manipulated on the spot, the logs are checked for intrusion and then detected, after which all the changes can be undone.

Tripwire is a free and open-source[1] software tool. It functions as a host-based intrusion detection system. It does not concern itself directly with detecting intrusion attempts in real time at the periphery of a computing system (as in network intrusion detection systems), but rather looks for and reports on the resultant changes of state in the computing system under observation

Intruders usually leave traces of their activities (changes in the system state). Tripwire looks for these by monitoring key attributes of files that should not change—including binary signatures, size, expected changes in size, etc.—and reporting its findings.

While useful for detecting intrusions after the event, it can also serve many other purposes, such as integrity assurance, change management, policy compliance, and more.

A Host-based Intrusion Detection System (HIDS), as a special category of an Intrusion-Detection System, focuses its monitoring and analysis on the internals of a computing system rather than on its external interfaces (as a Network Intrusion Detection System (NIDS) would do)

## Scope

1. Increase security
Tripwire software immediately detects and pinpoints unauthorized change-whether malicious or accidental, initiated externally or internally. Tripwire provides the only way to know, with certainty, that systems remains uncompromised.

2. Instill Accountability
Tripwire identifies and reports the sources of change, enabling IT to manage by fact. It also captures an audit trail of changes to servers and network devices.

3. Gain Visibility
Tripwire software provides a centralized view of changes across the enterprise infrastructure and support multiple devices from multiple vendors.

4. Ensure Availability
Tripwire software reduces troubleshooting time.

# THE ACTUAL WORKING OF THE TRIPWIRE SYSTEM

A HIDS will monitor all or part of the dynamic behavior and of the state of a computer system. Much as a NIDS will dynamically inspect network packets, a HIDS might detect which program accesses what resources and assure that (say) a word-processor hasn't suddenly and inexplicably started modifying the system password-database. Similarly a HIDS might look at the state of a system, its stored information, whether in RAM, in the file-system, or elsewhere; and check that the contents of these appear as expected.
One can think of a HIDS as an agent that monitors whether anything/anyone - internal or external - has circumvented the security policy that the operating system tries to enforce.

## 3.1 MONITORING DYNAMIC BEHAVIOUR

Many computer users have encountered tools that monitor dynamic system behavior in the form of anti-virus (AV) packages. While AV programs often also monitor system state, they do spend a lot of their time looking at who is doing what inside a computer - and whether a given program should or should not access one or another system resource. The lines become very blurred here, as many of the tools overlap in functionality.

## MONITORING STATE

The principle of operation of a HIDS depends on the fact that successful intruders (crackers) will generally leave a trace of their activities. (In fact, such intruders often want to *own* the computer they have attacked, and will establish their "ownership" by installing software that will grant the intruders future access to carry out whatever activity (keyboard logging, identity theft, spamming, botnet activity, spyware-usage etc.) they envisage.)
In theory, a computer user has the ability to detect any such modifications, and the HIDS attempts to do just that and reports its findings. Ideally a HIDS works in conjunction with a NIDS, such that a HIDS finds anything that slips past the NIDS.

Ironically, most successful intruders, on entering a target machine, immediately apply best-practice security techniques to secure the system which they have infiltrated, leaving only their own backdoor open, so that other intruders can not take over *their* computers. (Crackers are a competitive bunch...) Again, one can detect (and learn from) such changes.

TECHNIQUE

In general a HIDS uses a database (object-database) of system objects it should monitor - usually (but not necessarily) file-system objects. A HIDS could also check that appropriate regions of memory have not been modified, for example - the system-call table comes to mind for Linux, and various vtable structures in Microsoft Windows.

For each object in question a HIDS will usually remember its attributes (permissions, size, modifications dates) and perhaps create a checksum of some kind (an MD5 hash or similar) for the contents, if any. This information gets stored in a database for later comparison (checksum-database). Note that a matching MD5 hash does not provide a complete guarantee that an intruder or other unauthorised user has not tampered with the target file. Recent (2004) research has resulted in claims (still under debate) that the probability of such tampering may exceed what one might hope.

## OPERATION OF TRIPWIRE

At installation time - and whenever any of the monitored objects change legitimately - a HIDS must initialise its checksum-database by scanning the relevant objects. Persons in charge of computer security need to control this process tightly in order to prevent intruders making un-authorized changes to the database(s). Such initialisation thus generally takes a long time and involves cryptographically locking each monitored object and the checksum databases or worse. Because of this, manufacturers of HIDS usually construct the object-database in such a way that makes frequent updates to the checksum database unnecessary.

Computer systems generally have many dynamic (frequently changing) objects which intruders want to modify - and which a HIDS thus should monitor - but their dynamic nature makes them unsuitable for the checksum technique. To overcome this problem, HIDS employ various other detection techniques: monitoring changing file-attributes, log-files that decreased in size since last checked, and a raft of other means to detect unusual events.

Once a system administrator has constructed a suitable object-database - ideally with help and advice from the HIDS installation tools - and initialized the checksum-database, the HIDS has all it requires to scan the monitored objects regularly and to report on anything that may appear to have gone wrong. Reports can take the form of logs, e-mails or similar.

PROTECTING THE HIDS

A HIDS will usually go to great lengths to prevent the object-database, checksum-database and its reports from any form of tampering. After all, if intruders succeed in modifying any of the objects the HIDS monitors, nothing can stop such intruders from modifying the HIDS itself - unless security administrators take appropriate precautions. Many worms and viruses will try to disable anti-virus tools, for example. Sadly, a lot of them succeed in doing so.

Apart from crypto-techniques, HIDS might allow administrators to store the databases on a CD-ROM or on other read-only memory devices (another factor militating for infrequent updates...) or storing them in some off-system memory. Similarly, a HIDS will often send its logs off-system immediately - in some instances via one-way communications channels, such as a serial port which only has "Transmit" connected, for example.

One could argue that the trusted platform module comprises a type of HIDS. Although its scope differs in many ways from that of a HIDS, fundamentally it provides a means to identify whether anything/anyone has tampered with a portion of a computer. Architecturally this provides the ultimate (at least at this point in time) host-based intrusion detection, as depends on hardware external to the CPU itself, thus making it that much harder for an intruder to corrupt its object and checksum databases.

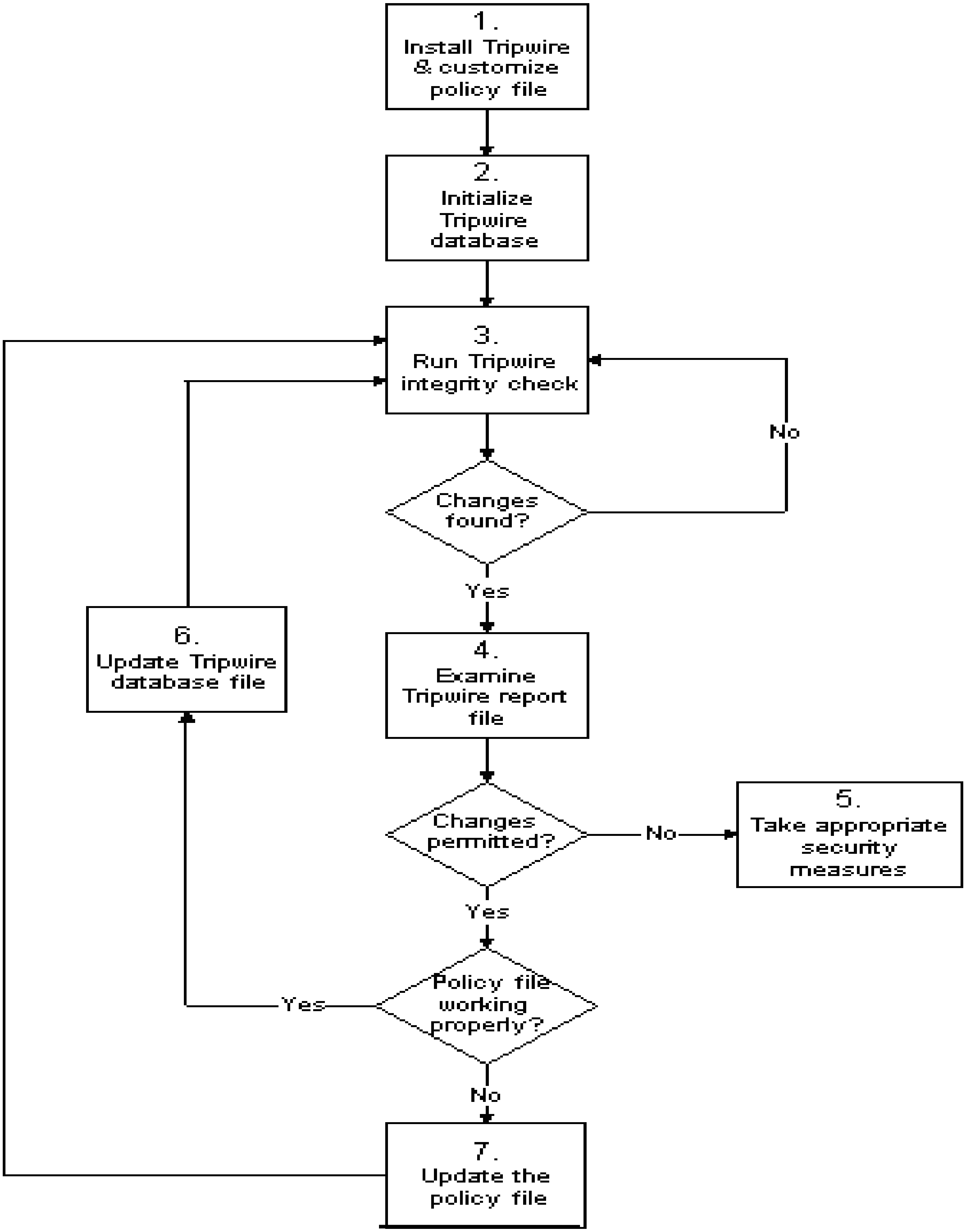
1.
Install Tripwire & customize policy file
2.
Initialize Tripwire database
3.
Run Tripwire integrity check
No
Changes found?
Yes
6.
Update Tripwire database file
4.
Examine Tripwire report file
Changes permitted?
No
5.
Take appropriate security measures
Yes
Yes
Policy file working properly?
No
7.
Update the policy file

FIG.1: FLOW CHART SHOWING THE WORKING OF TRIPWIRE

1. Install Tripwire and customize the policy file

Install the Tripwire software into the system and then specify the files to be checked by writing the policy files. Using the version 4.0 writing the policy file is made very easy.

2. Initialize the Tripwire database

The database is initialized with the important key attribute in the file to be checked. Build database of critical system files to monitor based on the contents of the new, signed Tripwire policy file.

3. Run the integrity check

Compare the newly created Tripwire database with the actual system files, looking for missing or altered files, according to the integrity check timing specified by in the policy file for different files that are to be monitored.

4. Examine the Tripwire report file

View the Tripwire report file to note any integrity violations.

5. If unauthorized integrity violations occur, take appropriate security measures

If monitored files have been altered inappropriately, the system administrator have to take immediate action, you can either replace the original files from backup copies reinstall the program, or completely reinstall the operating system.

6. If the file alterations were valid, verify and update the Tripwire database file.

If the changes made to monitor files are intentional, edit Tripwire's database file to ignore those changes in subsequent report.

7. If the policy file fails verification, update the Tripwire policy file

To change the list of files Tripwire monitors or how it treats integrity violations, update the supplied policy file, regenerate a signed copy, and update the Tripwire database.

# TRIPWIRE MANAGER

Tripwire Manger is a fully functional, cross platform management console that allows system and security professionals to easily manage all installations of Tripwire for Servers software across an enterprise network. Tripwire Manager eliminates the need to manually monitor multiple discrete network platforms and point solutions. Instead, IT professionals have a comprehensive view of data integrity status from a single centralized console. Tripwire Manager also enables you to view and analyze reports from installations of Tripwire for Servers. With Tripwire Manager you can retrieve an integrity system, which is made up of the configuration, database, policy, local and site key, from a single “golden” machine which can then be distributed to as many servers that need to be compared against this snapshot. In version 4.0 of the Tripwire Manager you can create and modify policy files by using graphical policy editor. This GUI will scan the remote file system of a Tripwire for Servers installation and provide you with an easy mechanism for editing or creating a policy file without having to know the policy file syntax. Tripwire Manager can manage the functions of Tripwire for Servers on up to 2500 machines.

Adding or removing recognition of Tripwire for Servers is easy to do from within the Tripwire Manager console. All you need to know is host name, IP address and a port number. The Tripwire for Servers database can be updated by using the database update mode within Tripwire Manager. All communication between Tripwire Manager and installation of Tripwire for Servers takes place using Secured Socket Layer (SSL) technology with 168-bit Triple DES encryption. To protect against unauthorized modification, important files on each Tripwire for Servers installation are stored in a binary-encoded and signed form. Database, policy, configuration, and report files generated by the integrity assessment are protected by using El Gamal asymmetric cryptography with a 1024-bit signature.

There are mainly two types of Tripwire Manager

- Active Tripwire Manager
- Passive Tripwire Manager

A user can have more than one Tripwire Manager managing the same set of Tripwire for Servers machines. However, only one can be in active mode and have complete management control of Tripwire for Servers machines. This active Tripwire Manager gives a user the ability to update the database, schedule integrity checks, update and distribute policy and configuration files and view integrity reports. The other Tripwire Manager is in a passive mode. The passive mode only allows these Tripwire Manager to view the status of the machines and integrity reports. Once the active Tripwire Manager shuts down, the next time the passive Tripwire Manager pings the Tripwire for Servers machine it connects as an active Tripwire Manager. If more than two passive Tripwire Managers, the one that connects first to the Tripwire for Servers machine after the active Manager has hut down becomes the active Manager.

# TRIPWIRE FOR SERVERS

Tripwire for Servers is software that is exclusively used by servers. This software can be installed on any server that needs to be monitored for any changes. Typical servers include mail servers, web servers, firewalls, transaction server, development server etc. Any server where it is imperative to identity if and when a file system change has occurred should be monitored with tripwire for servers. For the tripwire for server's software to work two important things should be present – the policy file and the database.

The tripwire for Servers software conducts subsequent file checks, automatically comparing the state of the system with the baseline database. Any inconsistencies are reported to the Tripwire Manager and to the host system log file. Reports can also be emailed to an administrator. If a violation is an authorized change, a user can update the database so changes no longer show up as violations.

FLEXIBLE POLICY LANGUAGE

The power behind Tripwire technology lies in its highly configurable policy language. The policy file is how a user directs Tripwire for Servers to monitor specific files or directories. The flexible policy tool can be customized to fit the needs of each and every server. With the release of version 4.0, policy file creation has become even easier. From Tripwire Manager 4.0, a graphical policy editor allows users to select the files and directories, along with the scanning options that need to be monitored in each integrity check. Included in the products are default policy files for each supported operating system to make it easy for the user to set up which files should be monitored. In the latest version, wildcard application is also supported which enables users to add objects to the policy file by specifying the file type. In 4.0, objects listed in the policy file but not present on the user's machine will no longer be categorized as violations. By only showing violations caused by added, deleted or changed files, report noise is greatly reduced. Tripwire policy languages also allow you to group objects around easy-to-understand rule names and then prioritize them.

The snapshot and the policy file are cryptographically signed with 168-bit Triple DES encryption algorithm that detects any unauthorized tampering. The default policy file also monitors the tripwire binary files, in short, it uses tripwire itself to monitor the tripwire.

In the latest version 4.0 in addition to reporting the administrator which file has changed, when the change occurred and where the change took place it also to some extend determines who made these changes. Tripwire for Servers track the identity of who made the change by correlating the information from the operating system's event and audit log with the integrity information that is detected by Tripwire for Servers. It uses this information to provide the identity of who made a certain change. Since we rely on the operating system to gather this information, the product only captures the "who" information from the operating system that track this. Linux and FreeBSD do not track this information. This feature is called Event Log Correlation.

Each Tripwire for Servers report details when the database was last updated, providing a quick benchmark of if or when detailing if the data files have been replaced. In order to replace these files, an attacker requires root or administrator level privileges and must know where Tripwire for Servers has been installed. On a properly secured system, gaining this level of access takes time and leaves physical evidence behind for Tripwire for Servers to detect prior to the system being compromised. Methods for reducing the risk of an intruder being able to replace a Tripwire for Servers installation include:

- Hiding the application by renaming configuration, data, and binary files and installing to a hidden location.
- Installing Tripwire for Servers to a read-only partition such as a CD-ROM.

# TRIPWIRE FOR NETWORK DEVICES

Router, switch, and firewall configurations are critical to overall network operation. Unwanted changes to configuration files can result in downtime and security issues and waste hours of staff time searching for the cause. Tripwire for Network Devices monitors the integrity of routers, switches and firewalls-network devices that communicate network traffic within and between networks. It helps network administrator answer the question, “Has the state of my network devices changed from a known, trusted state? If so, how?” Problem’s with one network device can seriously disable an organization’s entire network. Network downtime can result in lost revenue and lost customer confidence. Manual processes to secure your network devices are available and important. Tripwire for Network Devices augments and helps guarantee that the security of your network devices remains in tact. With Tripwire for Network Devices, downtime is minimized. Network administrators can use Tripwire for Network Devices to quickly investigate and isolate changes and restore changed configuration files within minutes of an alert.

Tripwire for Network Device includes six primary functions:

- Automatic notification of changes to your routers, switches and firewalls
- Automatic restoration of critical network devices
- Audit trail from log files and change reports – ideal for internal/external network audits.
- Baseline archiving and configuration file “Hot Back-up” solution
- Heterogeneous support for today’s most commonly used network devices
- Sets a framework for autonomic recovery

Tripwire for Network Devices does not provide real time monitoring. It checks your network devices for change according to schedule you set. Device passwords stored by the software are protected by robust 1024-bit Blowfish cryptography. The software has four user authorization levels:

- “Monitors” are allowed only to monitor the application. They cannot make changes to Tripwire for Network Devices or to the devices that the software monitors.
- “Users” can make changes to Tripwire for Network Devices, such as add routers, switches. Groups, tasks, etc., but they cannot make changes to the devices it monitors.
- “Powerusers” can make changes to the software and to the devices it monitors.
- “Administrator” can perform all actions, plus delete violations and log messages as well as add, delete, or modify user accounts.

Tripwire for Network Devices maintains a log of all significant actions, including adding and deleting nodes, rules, tasks, and user accounts. All log entries include a time and date, and identify the user who initiated the process. The log entries cannot be modified by anyone other than the administrator and can be copied and pasted into a text file so you can create a library of log activities that are ideal for network audits.

Device password are stored by the software are protected by robust 1024-bit Blowfish cryptography. Tripwire for Network Devices has been tested and can monitor thousands of network devices. Tripwire for Network Devices software has been tested up to 6,000 network devices running integrity checks every 10 minutes. With correct configuration, the software can monitor more than 6,000 devices at one time.

# HOW TO INSTALL AND USE THE TRIPWIRE SYSTEM

The following steps should be taken to properly install, use and maintain Tripwire:

- Install Tripwire and customize the policy file — If not already done, install the tripwire RPM. Then, customize the sample configuration (/etc/tripwire/twcfg.txt) and policy (/etc/tripwire/twpol.txt) files and run the configuration script (/etc/tripwire/twinstall.sh).
- Initialize the Tripwire database — Build a database of critical system files to monitor based on the contents of the new, signed Tripwire policy file (/etc/tripwire/tw.pol).
- Run a Tripwire integrity check — Compare the newly-created Tripwire database with the actual system files, looking for missing or altered files.
- Examine the Tripwire report file — View the Tripwire report file using twprint to note integrity violations.
- Take appropriate security measures — If monitored files have been altered inappropriately, you can either replace the originals from backups or reinstall the program.
- Update the Tripwire database file — If the integrity violations are intentional and valid, such as if you intentionally edited a file or replaced a particular program, you should tell Tripwire's database file to not report them as violations in future reports.
- Update the Tripwire policy file — If you need to change the list of files Tripwire monitors or how it treats integrity violations, you should update your sample policy file (/etc/tripwire/twpol.txt), regenerate a signed copy (/etc/tripwire/tw.pol), and update your Tripwire database.

# HOW TO USE TRIPWIRE

Tripwire is a file integrity checker for UNIX/Linux based operating systems and works as an excellent intrusion detection system. It will not prevent an intrusion; for this see my previous articles on setting up firewalls and securing a Linux distribution for help.

The idea behind Tripwire is quite simple: it first creates a "baseline" database of the state of the files and directories on your system and then on subsequent runs it compares the current state of the files and directories against this baseline identifying any deletions, additions or changes. The files and directories to be checked are decided by a "policy" file. This file also defines what attributes to compare; this can include access, inode and modification timestamps, owner and group IDs, permissions, file size and type, MD5 and SHA hash values, etc.

In this article I will guide you through the process of getting and installing Tripwire, configuring it and setting it up to run on a daily basis. In the final section I will mention a few additional steps you can take to ensure the integrity of your Tripwire database and thus your file system.

2. Acquiring and Installing Tripwire

The easiest method of installing Tripwire is to use a vendor supplied package (I have checked and these are available for RedHat/Fedora Core, SuSE, Mandrakesoft and Debian). The advantages of using these are that the policy file will be already created and configured for the system you are using. Make sure to use official packages for your distribution to ensure they have not been trojaned.

If you cannot locate a precompiled package for your distribution, then you can download the latest source code from http://sourceforge.net/projects/tripwire/. The version available at time of going to press was 2.3.1-2. This version is dated March 2001 and when I tried to compile it on my system I got a myriad of errors. The sources do not use the autoconf/automake build system and this may be the main cause of the errors. I have decided to place the resolution of these problems outside the scope of this article given the availability of precompiled packages for many distributions.

3. An Overview of Tripwire's Files

The operation of Tripwire is controlled by a configuration file and a policy file; both of these files are encoded and signed before use for security reasons. These files *usually* reside in /etc/tripwire. The plain text versions are called twcfg.txt and twpol.txt, and the encoded and signed versions are called tw.cfg and tw.pol. The plain-text version of the configuration file contains key-value pairs including the following required variables (default values for my distribution shown):

```
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
```

The POLFILE, DBFILE and REPORTFILE dictate the locations of the policy file, the database file and the report file respectively. A report file is generated each time Tripwire

is used to check the integrity of the file system and its name is determined by both the hostname and current date. The SITEKEYFILE and LOCALKEYFILE variables hold the locations of the two key files; site keys are used for signing files that can be used on multiple systems within an organisation such as the policy and configuration files, while the local key is used for files specific to this system such as the database file.

Ensure that the $HOSTNAME environment variable is correctly set to your system's hostname before using any of Tripwire's commands. Also, the HOSTNAME variable in twpol.txt must be set correctly so that it matches the system's hostname. Other configuration file values we will use are shown here followed by a description of each:

```
EDITOR              =/bin/vi
MAILNOVIOLATIONS      =true
EMAILREPORTLEVEL      =3
REPORTLEVEL          =3
MAILMETHOD           =SENDMAIL
MAILPROGRAM           =/usr/sbin/sendmail -oi -t
```

When updating the database after files have been added, removed or altered, a "ballot-box" styled form must be completed by placing an 'x' opposite the files which we have changed and do not indicate an intrusion; this variable sets the editor to use for this process.

MAILNOVIOLATIONS

Tripwire e-mails a report whenever a violation was found. This option tells Tripwire to always e-mail a report whether a violation was found or not. This is useful as it shows the system administrator that Tripwire is running as expected.

EMAILREPORTLEVEL and REPORTLEVEL

The amount of information Tripwire includes in its report file and e-mail. Valid values range from 0 to 4 with the default being 3.

MAILMETHOD and MAILPROGRAM

The mail method can either be SMTP (in which case additional variables have to be set to indicate the SMTP host and port) or SENDMAIL (in which case we include the MAILPROGRAM variable).

There are a number of other options and these are explained in the man page: TWCONFIG(4).

Creating your own policy file is a long and tedious task that is also outside the scope of this article. If you get a packaged version of Tripwire for your distribution then the policy file should already be created. The policy file is essentially a list of rules and associated files which should be checked by Tripwire; the rules indicate the severity of a violation.

The text version of the file itself is quite readable and is worth a look to fully understand how Tripwire works

## ADVANTAGES OF TRIPWIRE

Tripwire Integrity Management solutions give organizations visibility into service affecting changes and, in the process, increase security, instill process accountability, and improve system availability.

1. Increase security

Tripwire software immediately detects and pinpoints unauthorized change-whether malicious or accidental, initiated externally or internally. Tripwire provides the only way to know, with certainty, that systems remains uncompromised.

2. Instill Accountability

Tripwire identifies and reports the sources of change, enabling IT to "manage by fact." It also captures an audit trail of changes to servers and network devices.

3. Gain Visibility

Tripwire software provides a centralized view of changes across the enterprise infrastructure and support multiple devices from multiple vendors.

4. Ensure Availability

Tripwire software reduces troubleshooting time, enabling rapid discovery and recovery. Immediate detection of change enables the fastest possible restoration back to a desired, good state.

# Limitations of Tripwire

1. History Mechanism
The single most important time efficiency issue with Tripwire is the lack of a report history mechanism, which would drastically reduce the number of reports.

2. Report Formats
Although the commercial Tripwire product has five report formats, none of them offers a maximally-abbreviated single-line format that provides violation type, filename, and changed attribute keys in a single line.

3. Lack of Regular Expressions
The Tripwire policy file allows complete exclusion or lower security policies on directory trees.

4. E-Mail Report Minimization
Tripwire now allows e-mail reporting to go to different addresses for different portions of a machine's file systems.

5. Ease of Maintenance
Tripwire database and policy file maintenance are made easier if the Tripwire admin does not have to remember argument switches and long filenames.

# Conclusion

Although having some limitations ;Tripwire is a reliable intrusion detection system. It is a software that can be installed in any type of system where damaged files are to be detected.

The main attractive feature of this system is that the software generates a report about which file have been violated, when the file have been violated and also what in the files have been changed. To some extend it also helps to detect who made the changes. New versions of Tripwire is under research and development. The latest version under research is the Tripwire for Open Source.

## References

- www.google.com
- www.wikipedia.com
- www.studymafia.org