OSSIM
Open Source Security Information Management

Last few years, Open Source softwares are widely adopted in I.T industry. Open Source software are most popular because free distribution and variety of features. OSSIM is integrated solutions of Open Source softwares like NTOP, Snort, Nessus, and Nmap. OSSIM is used for monitoring I.T infrastructure that includes network elements, Network traffic status, Service availability, Asset Inventory, IDS, security level of network elements.
About the Author

Vipul Ramani
Vipul Ramani is an associate of Open Source and Linux Practice and has expertise in different Open Source Infrastructure and security solution. He is one of the co-leads for Legacy Application to Linux Migration initiative and offerings. Vipul holds Bachelor’s degree in Electronics from Sardar Patel University India and has five years of experience in IT industry.
Table of Contents

1. OSSIM - An Overview 3
2. OSSIM Key Driver 6
3. Reference 7
OSSIM – An Overview

IT Infrastructure management is essential for any IT company, since most corporate IT networks are mission-critical. Yet for many years, IT executives were resigned to a frustrating reality: they had no alternative to using a proprietary solution for robust IT monitoring and management functionality—although these commercial platforms have been widely criticized as being expensive, overly complex, and difficult to deploy and manage.

Industries always had the need for softwares to monitor their IT networks and today this requirement of Infrastructure monitoring software like NMS has increased many folds. While the need for an enterprise-class IT management solution is more acute than ever, Infrastructure teams now have a dramatically expanded set of options to meet this critical need. The change has come in the form of open source Infrastructure management solutions, which have rapidly matured to a level of robust functionality and reliability. Similar to Apache’s explosive rise to dominance in web servers, “Snort” is used as pattern detector, and “Nessus” is used for penetration testing for Internal and External networks. In an effort to cut costs and simplify their Infrastructure management systems, companies have only one choice—to rely on open source Infrastructure management products. That high profile firms have successfully adopted these systems provides concrete evidence that IT teams now have a viable and market-tested open source alternative to closed commercial systems.

Introduction

OSSIM is a distribution of open source products that are integrated to provide Infrastructure (LAN/WAN) monitoring and security monitoring over predefined networks. OSSIM comes under BSD License distribution. OSSIM is a cost effective solution in the area of monitoring network health and security of Small/enterprise network/hosts compared to all other propriety products.

OSSIM and its Functionality

OSSIM is used for LAN/WAN traffic monitoring and application availability including Uptime and Downtime of services such as Web servers, Database Servers, LDAP Servers, Radius Servers and so forth.

NMS

NMS stands for Network Management System. NMS manages a network (or a portion of the network segments or particular hosts) through a network management protocol such as SNMP.

Pattern Detectors

Pattern is used in majority of the traditional kind of detectors. One classical example of a pattern detector is the Intrusion Detection System (IDS). IDS is capable of detecting patterns defined using Signatures or Rules. OSSIM includes snort as Open Source IDS. OSSIM has an in-built ID. Any element in the network, such as a router, a workstation, a firewall and so forth, has some capacity for detection. So IDS can be tied to any network element to collect events from all network elements, to get a comprehensive view of the network.

Anomaly Detectors

Traditionally all the IDS products had to be configured to detect a set of predefined anomalies using patterns. Now, IDS products have also developed an ability to learn on their own. In this case the detection system need not be prompted as to what is good and what is bad for the system; it can learn on its own and alert us when behaviour deviates enough from what it has learnt is normal.

Centralisation and Normalisation

Centralisation and Normalisation are aimed at unifying Security Events from all network elements throughout the organization in a single format or using just one console. Primary requirement for any security product is to include a centralized dash-board to display the summary of networks segments or network elements. All security products normally have a capacity for centralized management using standard protocols. The same is achieved in OSSIM using forms of communication that are native to systems. Normalisation requires a
prioritisation

The priority of an alert should depend on the topology and inventory of the organization’s systems. The reasons are quite clear, as demonstrated by the following examples:

If a machine is running the Linux operating system and the Apache web server receives an alert about an attack on Microsoft IIS, the alert should be de-prioritised.

If a user makes a suspicious connection to a server, the system should:

- Assign it maximum priority if the user is external to the network and attacking the client database.
- Assign it low priority if the user is internal to the network and attacking a network printer.
- Discard it if the user is someone who normally tests development servers.

Risk Assessment

The importance of Risk Assessment given to an event depends on these three factors:

- a. The value of the assets associated with the event
- b. The threat represented by the event
- c. The probability that the event will occur

Intrinsic Risk

The factors mentioned above are the building blocks for the traditional definition of risk: a measure of the potential impact of a threat on assets given the probability that it will occur. Traditionally, risk assessment is concerned with intrinsic risks, or latent risks; in other words, risks that an organization assumes by virtue of both the assets it possesses for the purpose of developing its business and circumstantial threats to those assets.

Immediate Risk

OSSIM is capable of measuring real-time risk associated with the current situation. The measurement of risk is weighted by the damage it would wreak and the probability that the threat is occurring in the present. That probability, which is a derivative of the imperfection of our sensors, turns out to be nothing more than the degree of reliability of our sensors in detecting the potential intrusion-in-progress. Immediate risk denotes the state of risk produced when an alert is received and assessed instantaneously as a measure of the damage an attack would produce, weighted by the reliability of the detector that made the report.

Correlation

OSSIM uses Correlation function as an algorithm that executes an operation on input data (from Snort, Ntop, tcpdump) and returns output data. Correlation in OSSIM has two pre-defined monitors (monitor and report health of the network elements) and Detector (detects the changes in the network environment) elements that provide information to its correlation function.

The two methods in correlation are:

1) Correlation using sequence (pre-define) of events: This method is followed by pre-defined definition of attack related to pattern and behaviours, for example, TCP-SYN attack on web server/Mail server.
2) Correlation using heuristic algorithms: These are not pre-defined attack events. We can define what attack definition Using different combination of parameters like source IP, destination IP, definite port/ pattern of TCP/IP etc. It is useful to detect unknown events, which are not already configured with the OSSIM package.
Monitors
OSSIM displays a risk monitor called a RISK METER that displays the values produced by the CALM algorithm. CALM stands for Compromise Attack Level Monitor and is an assessment algorithm that uses event accumulation with recovery over time and it takes a high volume of events as input while the output is a single indicator.

Forensic Console Control Panel
The forensic console provides access to all the information gathered and stored by the collector in databases. This console is a search engine that operates on the database, allowing the administrator to analyse security events in relation to all network elements of the network segment in a centralized manner.

Control Panel
The control panel allows defining a series of thresholds or objectives that the organization should meet. These thresholds are defined as either absolute or relative values such as degree of anomaly. The way information is displayed in the control panel is important, so it should be as concise and simple as possible. A flexible configuration may be introduced to this end, that shows only information that is relevant at that moment.

Case Studies
Organization requires its I.T infrastructure or(and) Data Center which includes WAN LAN network, Database, Mail server, different application servers and Intranet with different security level of access on different layers need to be monitored. Most secure segment has maximum level of security like 90 and DMZ (De-Militarized Zone) segment has level of security 60, LAN segment has level of security 70 and Internet Zone has 0 security level. Security level is defined based on data flow direction from low security segment to higher security level segment. 90 levels means very selected or specific data flow from lower security to most secure segment. Similarly 0 level means lowest level of security that indicates all data flow is allowed from Internet to this zone.

OSSIM is a modular tool that includes many open source tools integrated in order to help fulfil most of the aspects of network/system monitoring. It is also capable of generating different kinds of reports.

Various Alternatives Available In The Present Context
Now, a substantial number of tools are available with different features but tonnes of tools and effort to maintain those tools are required, to fulfil most requirements like monitoring network health and security of network.

Open Source: Promise Of Greater Technical Flexibility
OSSIM has three core technical characteristics that users claim make it agile and thus well-suited to the task of ensuring security, monitoring and managing heterogeneous Networks: the first characteristic is standards based and provides open interfaces; second, they are built on component architectures that are modular and configurable; and third, their source code is transparent and designed to be easily modifiable.

OSSIM includes the following major open source software:

1) SNORT : Open Source IDS
2) Nessus** : Measures security level of network elements.
3) NTOP : Shows statistics of network traffic and details analysis.
4) OpenNMS : Shows Service availability i.e UP-TIME/DOWN-TIME and assets/inventory management for existing infrastructure.
5) Nmap : Open Source Port-scanner.
6) ACID : PHP based Web-based front-end; provides various types of detailed report. The reports are related to malicious activity which are noticed by SNORT Sensors.

** Nessus for UNIX distribution
All the software mentioned above fall in the Open source category with the source codes being easily available. This characteristic gives open source vendors and service providers greater flexibility to design management systems tailored to complex IT infrastructure. This increased flexibility is particularly useful in managing homegrown applications and service oriented architectures.

**OSSIM KEY DRIVER**

**Cost Free: Source Code With Software**
Open Source software has the ability to customize to suit specific needs and to integrate easily with open source software or commercial software.

**Low Acquisition Cost**
OSSIM is open source software; the core software is essentially free. Clients pay only for enhancements, services, and support, deployment and support. OSSIM includes Open Source software modules like NTOP, SNORT, ACID, and Nessus. All of these fall under the category of GPL/BSD License.

**Low Scaling Costs**
NSM is particularly for monitoring activities and requires very little effort related to adjustment as new elements (for example, used applications, servers, and network equipment) are added to the network. Customers of commercial NMS tools quickly realise that as they expand their network, they also need to purchase licenses for more network device support or system add-ons to manage large scale Network elements. Unfortunately, the cost of those add-ons is often significant. At that point, they can either wait for low cost solutions or start in-house by writing code to the vendor’s proprietary API. Open Source software does not involve any licensing cost. Only fine tuning comes for a price, that is customization of an Open Source software involves a cost.

**Low Hardware Costs**
Open source products typically run on inexpensive, industry-standard boxes, further lowering overall costs.

**Open Source community is expanding:**
SourceForge.net Statistics
Registered Projects: 100,460
Registered Users: 1,079,020

There are many popular open source tools which are very famous and widely used. For example, Nagios for service and network monitoring, MRTG’s (Multi-Router Traffic Grapher) site gets 700 hits and 200 downloads per day, Rancid is change control management open source software to keep track of configuration changes in network elements like router, firewall, and switches on daily basis; Nmap is used for network scanning and discovery; Snot is used as an Open Source IDS, Ntop for network traffic analysis; Syslog NG for log file analysis; and Cacti for SNMP analysis and performance graphing. These products provide strong component functionality for an enterprise-class IT management solution and stand as enterprise software. For companies that need help either deploying, configuring, or customising Open Source solutions — or that simply want a fully integrated, supported solution—there is also a growing number of companies providing customised packaged open source solutions for IT management. They use Open Source software and modify them according to client requirements and there are even more firms offering expertise in integration and consulting services.

**Next Generation IT Vision: Open Source Frame Works**
Contributions from developers across the globe are making the Open Source Software/Frameworks more and more mature and stable. Companies have already started accepting Open Source products along with different versions of Commercial software. At the same time it is interesting to observe how different companies embrace this new category of open source solutions. Some will take a cautious, incremental
approach while other companies have already opted for a more aggressive, wholesale switch to an open source IT Infrastructure management system. There are clear signs of momentum behind open source IT Infrastructure management. The onus remains with the open source IT management vendors: To successfully translate this momentum into significant market share – a victory over the dominant proprietary platforms.

Reference

1) Homepage
   http://www.ossim.net

2) Mailing List
   http://sourceforge.net/forum/?group_id=86016
About Open Source & Linux Practice
From understanding business pain areas, recommending and implementing solutions to providing support, the OSL practice at TCS helps enterprises to overcome the challenges moving to Open Source, achieve tangible results and optimize the Total Cost of Ownership (TCO). The OSL practice offers secure and scalable solutions, built around Linux & Open Source, that cover Application Development, Re-engineering, Migration, Product Porting, Application Consolidation and Kernel Programming.

About Tata Consultancy Services
Tata Consultancy Services (TCS) is among the leading global information technology consulting, services and business process outsourcing organizations. Pioneer of the flexible global delivery model for IT services that enables organizations to operate more efficiently and produce more value, TCS focuses on delivering technology led business solutions to its international customers across varied industries.

For more information contact
Rakhi Gupta
Tata Consultancy Services Ltd
Akruti Business Port
Road No 13, MIDC
Andheri (East)
Mumbai 400093,
India

Phone: +91-22-5660 6311
Fax: +91-22-5660 6855

Email: linux.practice@tcs.com
Website: www.tcs.com