BULETINUL Universității Petrol – Gaze din Ploiești	Vol. LX No. 2/2008	53-58	Seria Matematică - Informatică - Fizică

Managing Security Monitoring in Enterprise Networks

Iustin Priescu[*], Sebastian Nicolăescu[**]

[*] Universitatea Titu Maiorescu, București
e-mail: iustin.priescu@utm.ro

[**] Verizon Business, New York, USA

Abstract:

A significant number of high profile cases of malicious software threats and incidents that have dominated media reporting for years have served to raise awareness and determine most businesses to invest time and resources into defending against this prevalent security issue. Security monitoring has gained support being regarded as an essential component for managing and improving the security of network infrastructures. The primary goal of a security monitoring system is to help identify suspicious events on a network that may indicate malicious activity or procedural errors. This paper presents the major security monitoring types in current enterprise networked environments.

Key words: *security, monitoring, detecting intrusions, correlation model*

Compliance Monitoring

Ensuring compliance starts with a corporate policy that reflects the necessary requirements for supporting an organisation's internal policies and applicable external regulations. The current compliance process consists mainly of three parts – the security administration staff monitoring its own efforts, the internal audit division of the organisation monitoring compliance with the security policy and standards, and external independent auditors monitoring the organisation in light of all appropriate regulatory and internal standards.

If current security solutions are focused on providing an automated support for handling alerts within the network and compliance process is driven by laws and regulations, the security approaches in the near future would be based on proactive components that continuously checks the network and systems, and provide a self learning mechanism through the handled alerts, attacks and other critical events. In this new environment, security issues will be handled by all elements of the network according to their abilities.

POSITIF (Policy-based Security Tools and Framework) proposes a security framework that checks the compliance a continuous basis and monitors security events against the policy. The framework needs two descriptions as an input: Security policy (security needs of the network) and description of all elements in the networks, including the security capabilities of each node.

The *security checker* module provides a sort of measurement of the actual level of security achieved by the policy given the network architecture. *Configuration engine* loads the desired configuration into the various elements (firewalls, switches, routers, etc).

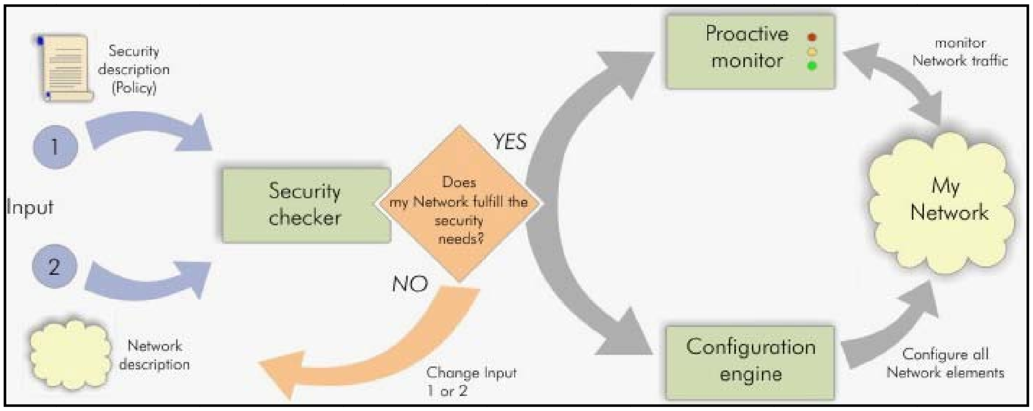

Fig. 1. POSITIF Framework

The *Proactive Security Monitor* (PSM) checks permanently the network for any behaviour that violates the deployed security policy. It does not only collect the events through sensors, but it also compares monitored data against the policy.

This method allows the detection of even unknown attack signatures. If an event is monitored the output will be an alarm with certain severity. Also semiautomatic or automatic reactions can be enforced. If a security violation is detected an updated security policy will be deployed either to the full system or part of the targeted system.

PSM also tests the proper behaviour of the enforced policy by sending dummy attacks to a part or the network and verifies the result of the attack.

Vulnerability Monitoring

The identification of vulnerabilities on networked systems is part of risk identification. It is important to monitor the number and type of system vulnerabilities so that the organization understands the security risk to these systems from an external or internal threat.

Unfortunately, identifying vulnerabilities once does not suffice when managing risk due to the following reasons:

- Changes to the number of vulnerabilities on existing systems need to identified.
- New systems come online and the vulnerabilities on these systems must be identified.
- New vulnerabilities are discovered that may affect existing systems.

The vulnerability picture for organizations is, therefore, constantly changing. A single snapshot of the vulnerabilities would be an insufficient evaluation of the risk to the organization.

The vast majority of *software vulnerabilities* are corrected by the vendors through the release of patches. By checking the software patch state on the system, one can identify which vulnerabilities the system is likely to be vulnerable to. Alternatively, one can check for each of the vulnerabilities and see if the system is in fact vulnerable. A combination of the two techniques is usually the best course of action.

Incorrect configurations can also cause vulnerabilities. Some configuration issues are part of configuration policies and procedures, but some parts of the system configuration may not be covered by the organization's policy.

For example, very few Web server configuration procedures specifically state that directory browsing should be turned off (usually this is understood by the administrators and they do it as a matter of course). Configuration problems can be operating system-related (such as inappropriate services left running) or they can be application-related.

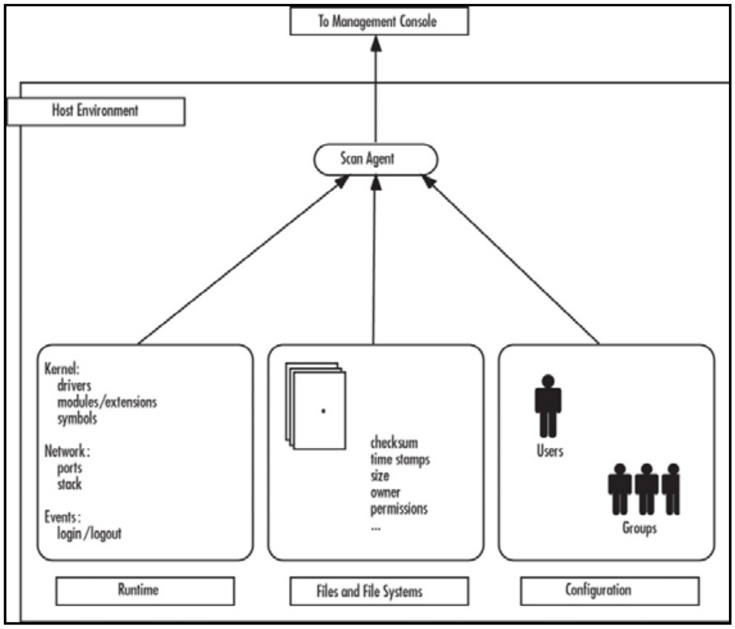

Fig. 2. Functional overview of system security monitoring

System Security Monitoring

System security monitoring (SSM) is the recurring assessment of a system's environment based on a known good state or policy. The overall goal is to detect and report on changes in the environment. A system can be a user's PC, a corporate e-mail or Web server, a production build system, a router or a switch.

As shown in figure 2, system's environment can be broken down into three categories: files, configurations, and runtime. Files are the most obvious and include the content and attributes associated with individual files as well as the file systems themselves.

The configurations of an environment are higher-level elements such as users and groups, access control, configurations for services, and basically anything that dictates the initial state of the system. The runtime involves the dynamics of a running system such as the state of a network stack (e.g., open ports), user login/logout activities, kernel state (e.g., extensions, services, drivers), system resources such as memory, and the running process table.

System security monitoring concept is related to host intrusion detection systems (HIDS). While HIDS purpose is to detect an attack or an intrusion, SSM is concerned with any changes to the environment that violate security policies.

The benefits of system monitoring would be: maintaining records of change activity for later analysis, detecting internal attacks, detecting intrusions, and forensics support.

Network Security Monitoring

Network Security Monitoring (NSM) is the collection, analysis and escalation of indications and warnings based on network traffic to detect and respond to policy violations (intrusions). The process of monitoring network traffic and network security events focuses on threats and actions that precede compromise.

The primary group of data that can be collected and analyzed to determine and validate the intrusions is the network traffic data. Based on the level of details, the network traffic data available for analysis can be: full content traffic data (it represents the complete raw network packet data captured by sensors), session traffic data (also known as flow or stream - is a summary of packet exchanges between two entities), statistics traffic data (represents a synthesis of network traffic over a time interval).

The second group is formed by security event data. It is generated by networked entities while processing the network traffic addressed to them or visible to them.

An example of monitoring solution for enterprise networks is OSSIM (Open Source Security Information Management). It is based on open source products that are integrated to provide an infrastructure for security monitoring.

OSSIM objective is to provide a framework for centralizing, organizing, and improving detection and display for monitoring security events within the organization.

The *detection components* of the first layer collect security events from all critical systems in order to achieve a comprehensive view of the network.

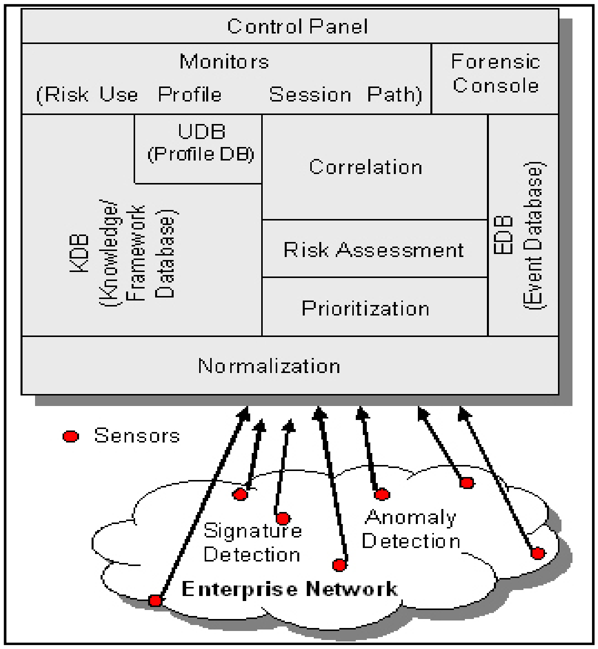

Fig. 3. OSSIM Architecture

The second layer, *normalization and aggregation*, is aimed at unifying security events from all critical systems throughout the organization in a single format on just one console. All security products normally have a capacity for centralized management using standard protocols; hence, aggregation is simple using these protocols. OSSIM attempts to avoid regular use of agents and instead use forms of communication that are native to systems.

Prioritization component evaluates the importance of the alerts in relation to the organization's environment, which is described in a knowledge base for the network comprised of: an inventory of machines and networks (identifiers, operating systems, services, etc.), and an access policy (whether access is permitted or prohibited, and from where to where).

Generally, the importance associated to an event depends on the following three factors which are the building blocks for the classical definition of *risk*: the value of the assets associated with the event, the threat represented by the event, the probability that the event will occur.

OSSIM *correlation model* has the following objectives:

- Develop specific patterns for detecting the known and detectable
- Develop non-specific patterns for detecting the unknown and the undetectable
- Provide an inference machine that can be configured using interrelated rules and that has the ability to describe more complex patterns
- The ability to link sensors and monitors recursively to create more abstract and useful objects
- Develop algorithms for displaying a general view of the security situation

OSSIM *monitors component* is monitoring the execution of processes from lower levels.

In addition to all the components described above, architecture has three databases: EDB (event database), KDB (knowledge database), UDB (profile database). The forensic console provides access to all the information gathered and stored by the collector. The last component, the control panel, allows the analyst to view the network security situation at a high level. It monitors a series of indicators that measure the state of the organization in relation to security.

Other Monitoring Types

Security relevant information useful in the correlation and analysis process can be obtained from other monitoring activities in the enterprise network like:

- *User activity monitoring* is an extra step that some organizations (eg. governmental, military, etc.) consider for reducing the risks associated with electronic communications and to protect corporate assets in the process. The surveillance scope on current products can range from e-mail and Internet connection monitoring, to keystrokes logging or screenshot captures.

- *Network traffic monitoring* as part of network management systems, may provide indications of unusual network activity patterns. Misuse or knowledge-based intrusion detection systems can use as input the information provided my network management systems.

- *Monitoring proactive alarms* of various applications running in the enterprise network can be used to determine in advance attacks on systems or network. Without proactive monitoring, network engineers usually learn about attacks from users calling in to report a network slowdown, high router CPU utilization or an automated ping reporting a site is unavailable.

- *Monitoring end user response time* is an external perspective of how the overall application performs from an end user view and identifies how long the response time is for an end user.

- *Monitoring overall system health* is important to understand the health of every system involved that includes web servers, application servers, databases, back end systems, and any other systems critical to the organisation.
- *Monitoring fault and performance* for infrastructure networks in conjunction with trending and forecasting algorithms may allow the real time automated threat assessment and detection of atypical or abnormal conditions, which can serve as indicators of potential threats.

Conclusions

Security is not a product; it is a continuous and dynamic process. Monitoring security would help organizations to minimize the window of exposure to risks and manage better their entire security process. The security monitoring based solutions are only successful to the extent that it integrates well with the people and processes of the organization that uses it. The operational model should have features that allow the security monitoring to be customized to people and processes within an organization.

References

1. Ionescu, E. - *MySQL pentru Începători*, Prentice-Hall, Englewood Cliff, 2002
2. Pavelescu, I., Dumbrăvescu, G. - *Managementul Resurselor Umane*, Editura Humanitas, Bucureşti, 1998
3. Patriciu, V.V., Priescu, I., Nicolăescu, S. - *Security Monitoring - An Advanced Tactic for Network Security Management*, COMMUNICATIONS 2006, Bucharest, 2006
4. Bejtlich, R. - *The TAO of Network Security Monitoring*, Addison- Wesley, 2005
5. Solomon, M.G., Chapple, M. - *Information Security Illuminated*, Jones and Bartlett Publishers, 2005
6. * * * - XYPRO Technology Corporation*,* *HP NonStop Server Security*, Digital Press, 2004
7. Buecker, A., Fulda, H.H., Riexinger, D. - *Deployment Guide Series: IBM Tivoli Security Compliance Manager*, IBM Redbooks, 2005
8. Wotring, B. - *Host Integrity Monitoring Using Osiris and Samhain*, Syngress Publishing, 2005
9. * * * - *Policy-based Security Tools and Framework*, POSITIF Project - http://www.positif.org/, 2007
10. * * * - *OSSIM*, OSSIM Project - http://www.ossim.net/ , 2007
11. * * * - Counterpane, *Managed Security Monitoring*, http://www.counterpane.com/msm.pdf, 2005
12. * * * - *Event Monitoring and Response on the Microsoft Network* (Technical White Paper), Microsoft, 2006

Managementul monitorizării securităţii în reţele de întreprindere

Rezumat

Un număr semnificativ de mare de cazuri de ameninţări cu software maliţios şi incidente de securitate au dominat mass-media de raportare, în scopul de a creşte gradul de conştientizare şi a determina cele mai multe întreprinderi să investească timp şi resurse în apărarea împotriva acestor predominante probleme de securitate. În prezent, securitatea monitorizării a câştigat sprijin, fiind considerată ca o componentă esenţială pentru managementul şi îmbunătăţirea infrastructurilor de securitate din reţea. Obiectivul principal al unui sistem de monitorizare de securitate este de a ajuta la identificarea evenimentelor suspecte din reţea care poate indica o activitate maliţioasă sau de erori de procedură. Lucrarea prezintă principalele tipuri de management al monitorizării securităţii în reţele şi medii de întreprindere.