TENABLE
Network Security®

Security Event Management

February 7, 2007
(Revision 5)

Table of Contents

TABLE OF CONTENTS 2

INTRODUCTION 3

CRITICAL EVENT DETECTION 3

LOG ANALYSIS, REPORTING AND STORAGE 7

LOWER TOTAL COST OF OWNERSHIP 7

CONCLUSION 9

ABOUT TENABLE NETWORK SECURITY 10

Introduction

Large enterprise networks generate an overwhelming amount of logs and security events. Firewalls, intrusion detection systems, web servers, authentication devices, and many other network elements contribute to more and more logs which need to be analyzed and produce actionable information.

Tenable Network Security, Inc. has developed a comprehensive strategy for enterprise security management. Our strategy leverages multiple event analysis technologies, as well as innovative communication and storage techniques. This paper examines Tenable's solutions and will highlight how they are effective in large enterprise networks.

Critical Event Detection

Tenable's philosophy for security event management is to focus on the generation of easily understood "actionable" events, and back that up with extremely scalable tools to navigate the flood of security logs. These actionable events can be sent to network operations centers, and can also be used as indicators of where to begin forensic analysis in the vast amount of stored logs.

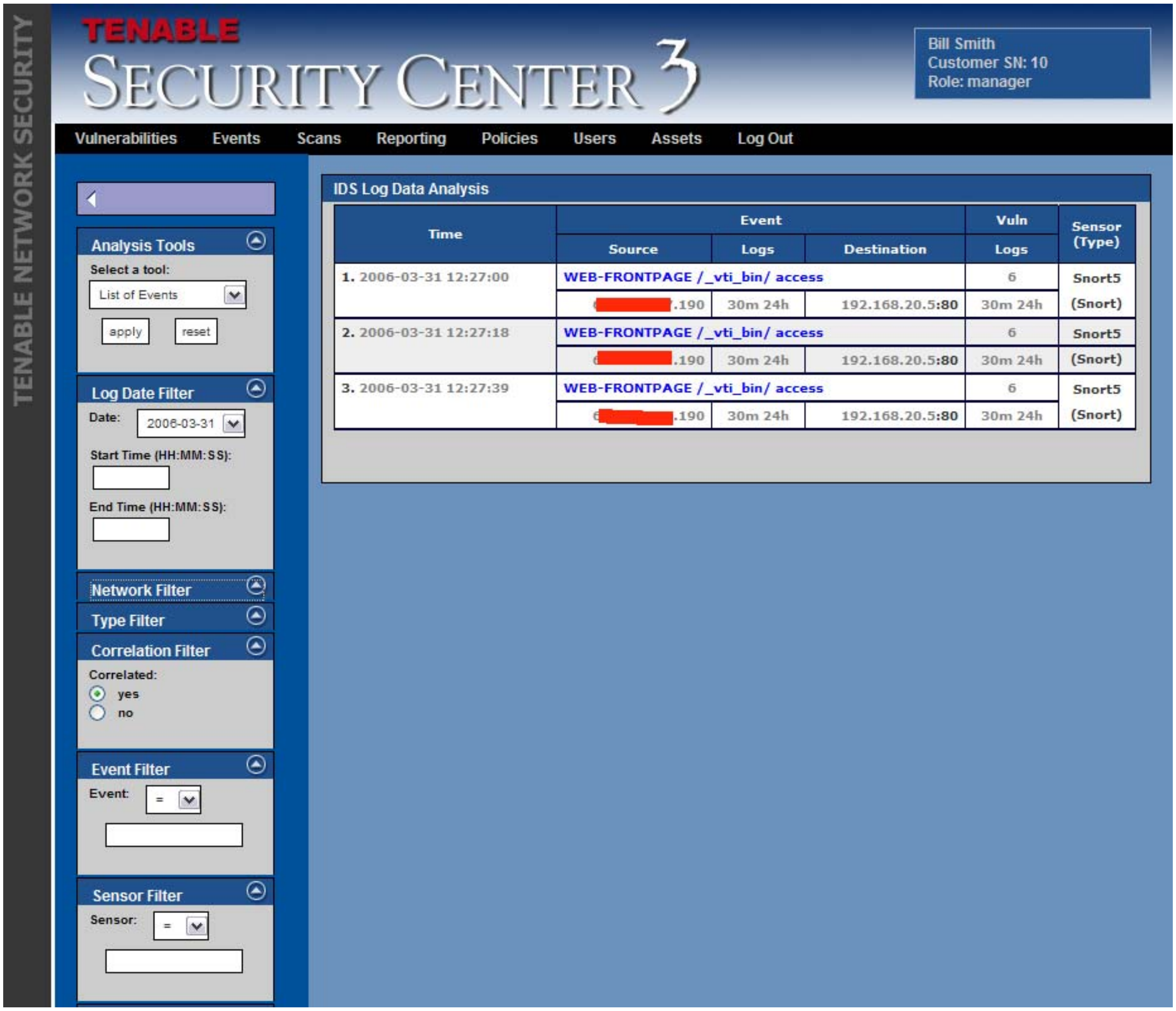
Vulnerability and IDS Event Correlation

Tenable has greatly simplified the intrusion detection "false positive" problem by performing real-time vulnerability to IDS event correlation with its Security Center. Modern network IDS devices generate enormous amount of alerts, most of which are real, but ineffective attacks. The Security Center has knowledge of the state of each server's vulnerabilities and automatically correlates known attacks against known vulnerabilities. This can reduce the amount of alerts from millions per day to dozens.

When a correlation occurs, a simple message that says a particular server has been attacked with a technique which is likely to succeed can be sent to system owners, operations people, and other places. This unique message can be used to build policies and procedures around events, regardless of the specific event type. It may not be obvious to an administrator what the nomenclature of a particular IDS event name is, but it is not hard to grasp that a critical attack may have occurred.

Security Center's technology is much more accurate than other forms of similar vulnerability correlation techniques because it can also make use of passively detected and host-based detected security information. Traditionally, most vulnerability correlation tools only make use of network scans which grow out of date quickly, and are often limited in scope. Security Center can import vulnerability data from the Passive Vulnerability Scanner. This is a sniffer which monitors network traffic 24x7 and detects new vulnerabilities and applications in real-time. Security Center can also manage the credentials required to "log" into UNIX and Windows servers to conduct host-based vulnerability checks. Information from network scans, passive analysis and host-based checks is then utilized to perform accurate vulnerability correlation with IDS events.

Below is a screen shot of the Security Center which shows IDS events from the Snort intrusion detection system that have been correlated with vulnerabilities detected by the Nessus Vulnerability Scanner:



Bill Smith
Customer SN: 10
Role: manager

Select a tool: List of Events

Date: 2006-03-31

Start Time (HH:MM:SS):

End Time (HH:MM:SS):

Correlated:
● yes
○ no

Event: =

Sensor: =

IDS Log Data Analysis

Time	Event			Vuln	Sensor (Type)
	Source	Logs	Destination	Logs	
1. 2006-03-31 12:27:00	WEB-FRONTPAGE /_vti_bin/ access			6	Snort5
	[redacted].190	30m 24h	192.168.20.5:80	30m 24h	(Snort)
2. 2006-03-31 12:27:18	WEB-FRONTPAGE /_vti_bin/ access			6	Snort5
	[redacted].190	30m 24h	192.168.20.5:80	30m 24h	(Snort)
3. 2006-03-31 12:27:39	WEB-FRONTPAGE /_vti_bin/ access			6	Snort5
	[redacted].190	30m 24h	192.168.20.5:80	30m 24h	(Snort)

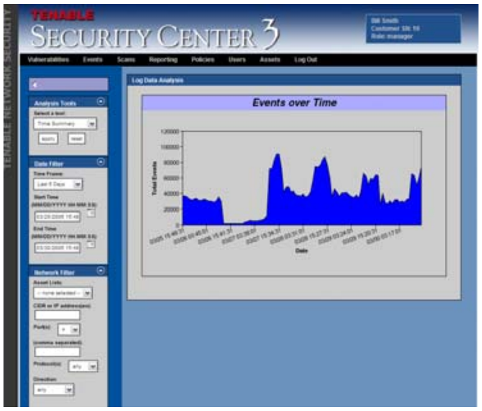
In the above image, the number 6 represents the number of vulnerabilities on the target port. Clicking on that number would bring the user to a listing of the vulnerabilities for just that server.

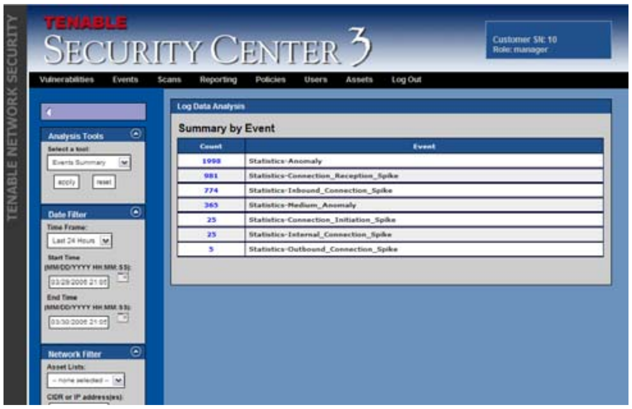
Statistical and Behavioral Anomaly Detection

Tenable has also simplified the process for automatically detecting trends and deviations from “normal” network activity. The Log Correlation Engine can be used to normalize and collect events from many different types of sources including sniffers, firewalls, servers, honeypots and authentication devices.

As the Log Correlation Engine receives these events, for each host on the network, it computes the normal event load and the amount of time the host is acting as a client or server. If there are swings in these “normal” loads, alerts can be generated. More interestingly, events that are only slightly statistically significant can be used as pointers to understand “normal” network behavior. This is a very important concept because network usage, load and communication flows often change on a daily basis.

Below are two screen shots of a graph of all Log Correlation Engine events and an image of just the statistically significant events detected by the Log Correlation Engine.





Log Data Analysis

Summary by Event

Count	Event
1998	Statistics-Anomaly
981	Statistics-Connection_Reception_Spike
774	Statistics-Inbound_Connection_Spike
365	Statistics-Medium_Anomaly
25	Statistics-Connection_Initiation_Spike
25	Statistics-Internal_Connection_Spike
5	Statistics-Outbound_Connection_Spike

In the event on the right, which was a snap shot of three days of network sessions and Windows 2000 server event logs, there are some easily recognizable peaks and valleys which correspond with business hours and off hours. However, this is a plot of all aggregate events and it does not capture anything out of the ordinary for specific servers. The graph on the right shows seven distinct spikes for the same time period. If desired, the user could "drill" into this display to browse the specific logs which contributed to generate these alerts. These spikes indicate changes in the flow of network data and can indicate alterations in user patterns, network load shifts and security events.

<u>Efficient and Scalable Business Rules Alerting</u>

Besides looking for statistical anomalies, the Log Correlation Engine can be programmed with any type of event alerting logic desired. Tenable has produced the Tenable Application Scripting Language (TASL) which is similar to JAVA and the Nessus Attack Scripting Language (NASL). TASL gives the Log Correlation Engine the ability to perform complex correlation between multiple events with any type of computational dependency. For example, each of these scenarios can be programmed in a simple TASL script:

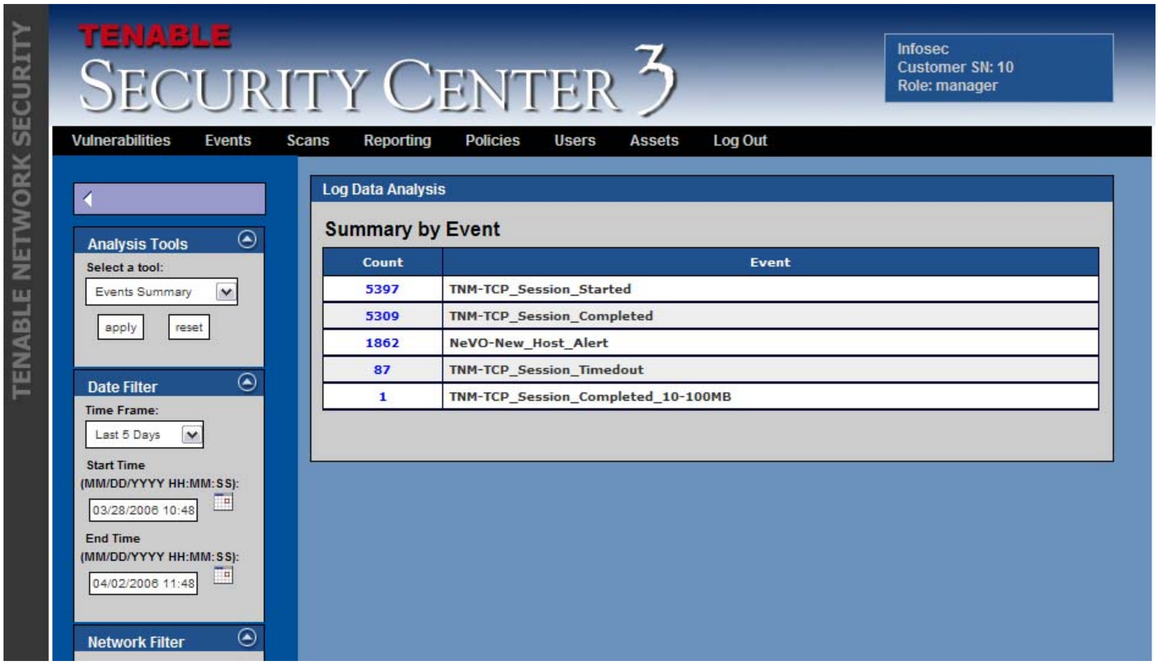
- Alerting if there have been more than 100 SSH login failures within 5 minutes.
- Alerting if there have been more than 10 authentication failures, a successful login, and a password change which is a common phishing technique.
- Alerting if two different types of NIDS (such as IntruShield and Snort) both see similar normalized attacks.
- Alerting if a specific network generates any outbound events.
- Detecting when "worm" IDS events have infected a host on the monitored network.
- Alerting on IDS events which have occurred.
- Alerting on large numbers of web "404" failures from a single host.
- Alerting on large numbers of TCP sessions (firewall or sniffed) from specific external networks which may indicate known hostile probing or scanning.

When TASL scripts generate new events, they can be fed back into the Log Correlation Engine for analysis by other TASL scripts, sent as an IDS event to the Security Center for alerting, sent as an email to a specific user list, or simply invoke a custom program.

TASL's performance is such that a typical Log Correlation Engine with dual CPUs and 2-4 GB of memory can handle management of 500 million normalized events and several dozen

TASL scripts. If necessary, multiple Log Correlation Engines can be used to distribute TASL analysis.

Below is a screen shot of the output of a TASL script designed simply to process the start and stop of TCP connections:



Infosec
Customer SN: 10
Role: manager

Analysis Tools
Select a tool: Events Summary
apply reset

Date Filter
Time Frame: Last 5 Days
Start Time (MM/DD/YYYY HH:MM:SS): 03/28/2006 10:48
End Time (MM/DD/YYYY HH:MM:SS): 04/02/2006 11:48

Network Filter

Log Data Analysis

Summary by Event

Count	Event
5397	TNM-TCP_Session_Started
5309	TNM-TCP_Session_Completed
1862	NeVO-New_Host_Alert
87	TNM-TCP_Session_Timedout
1	TNM-TCP_Session_Completed_10-100MB

The script considers the length of each TCP session and focuses on any connection longer then fifteen minutes, placing them into "buckets" such as a "15 Minute" session. This makes it very easy for an analyst to trend long TCP session activity and identify potential misuse. This script also identifies long TCP sessions which have low bandwidth activity that may be command and control channels for botnets, backdoors or compromised services.

Target Based Intrusion Detection

Previously mentioned, the Passive Vulnerability Scanner sniffs network traffic to discover vulnerabilities in real-time. As it discovers new hosts, new applications, and vulnerabilities it is also searching for evidence of likely compromised systems.

Tenable has programmed the Passive Vulnerability Scanner such that when it detects common applications, it searches outbound traffic for indications of compromise. For example, if the Passive Vulnerability Scanner observes an Apache web server on a particular host and port, it will look for the results of several common Apache exploits such as displaying the */etc/passwd* file and invocation of UNIX or Windows commands. These patterns are searched for, regardless of the exploit and regardless of any attack masking techniques used.

The alerts generated by the Passive Vulnerability Scanner are often only in the hundreds per day for even the busiest enterprise networks. This low "false positive" rate makes the data collected by the scanner useable not only by Tenable's Security Center and Log Correlation Engine, but by network management and operations consoles.

Log Analysis, Reporting and Storage

Intelligent Log Normalization and Storage

The Log Correlation Engine allows very easy configuration of which logs should be saved and which should be normalized. Simply put, the Log Correlation Engine can be configured to process events from close to 200 different log sources such as firewalls and operating systems.

When configuring the Log Correlation Engine, it is very easy to select what types of log sources exist, and what sort of events should be normalized. The Log Correlation Engine also has a mode where any log sent to it can be saved on the local disk, a second disk, or on network storage.

This is a very important concept because not all logs may be relevant to understanding your overall security posture, yet there may likely be regulatory requirements to store all logs. The Log Correlation Engine can be configured to solve both of these problems. For example, the Log Correlation Engine can be used to save all logs for 90 days, yet only normalize intrusion detection, firewall and Windows security events. This allows for efficient analysis of the security events, while still retaining all logs, including one not relevant to security for 90 days.

Ultra-High Speed Queries

Having a large amount of events is of little use if it takes 30 minutes to produce a “trending” report. Tenable’s approach is that all user interfaces for the Security Center and the Log Correlation Engine should handle close to 500 million normalized events and have any query complete in less than 10 seconds. This means that a user could sort events, find something of interest, and drill directly down into the actual log message in just a few clicks. It also means that a user can jump directly from an interesting intrusion event, to all log events (firewall, operating system, honeypot, etc.) concerning the attacker’s IP with one click.

Role Based Log Analysis

The Log Correlation Engine’s analysis performance also allows unique accounts to be configured that have limited access to the available data. For example, an account for all DNS administrators could be configured such that when they logged in, they would only be presented with logs that “touched” their servers.

This has several benefits. Foremost, during an incident, all of the relevant logs are available for immediate analysis. This includes historical events as well as those that occurred within the past 5 minutes. Although forensic log analysis is typically the job of the security expert, system administrators will often recognize aberrations in the logs which may otherwise go unnoticed. An additional benefit is that these logs are available for performance, diagnostics and troubleshooting. For example, having access to the firewall logs may help an email administrator troubleshoot the configuration of a high-availability server.

Lower Total Cost of Ownership

Compared to other security event management platforms of similar scope, Tenable's Security Center and Log Correlation Engine is easier to deploy, configure and make use of. Here are some of the reasons why:

Vulnerability Management and Compliance Tools

With the Security Center and Log Correlation Engine, your users will have one interface for vulnerability management, security event management and compliance reporting. Although this paper focuses on the virtues of Tenable's event management technology, our complete solution combines a variety of security practices. With this approach, there are many efficiencies which can be gained through common policy, reporting, training and incident response processes.

Ease of Installation

Both the Security Center and Log Correlation Engine are distributed as Linux "RPMs". This means that installation simply involves downloading the RPM, placing it on a server which runs Linux, and running a command to start the installation. A similar process is followed for upgrades. Most of our customers did not require us to go onsite to install our products, and many of them we have never met in person. Aside from an Apache web server and the Secure Shell server, we do not make use of any external software, which also minimizes installation troubles.

Simple Licensing Model

Tenable's licensing model for the Security Center and Log Correlation Engine are also very simple. This is an important feature because your network will change and your logging requirements will change with it.

The Security Center is simply licensed by the total number of servers for which you are performing security management. This could be 500 servers in a data center, or even 10,000 desktops. If you exceed your Security Center licenses, you can choose to purge some of your data or buy a larger license through a simple upgrade.

The Log Correlation Engine is a software solution deployed on a dedicated server. There is simply one price for the Log Correlation Engine and any combination of our log collection agents can be used with it. This is unlike some of our competitor's products which require each agent to be licensed, or the total amount of logs to be licensed. If your current Log Correlation Engine deployment grows inadequate, you can also procure additional Log Correlation Engine's for more processing power.

Works with Common Hardware

The Security Center and Log Correlation Engine are designed to run on typical 1U, one or two CPU x86 servers with 1 to 4 GB of memory. There is no requirement for RAID, high-speed disks, more than 4 GB of memory, or other extreme forms of hardware. However, if the Security Center or Log Correlation Engine is deployed on "premium" hardware solutions, they enjoy much higher performance.

Easily Extended

If the Log Correlation Engine does not contain rules or a desired feature, it can easily be extended. If you have a proprietary log format, it is very easy to write new Log Correlation

Engine rules to normalize those logs. If a certain type of alerting is also desired which is not performed by the Log Correlation Engine, it can be programmed with a TASL script.

Both of these features allow you to offer new types of logging capabilities for your organization. This can help transcend various technical and political boundaries normally encountered while conducting enterprise security.

Conclusion

Tenable's approach to security event management for large enterprise networks offers a number of advantages. Critical events can easily be recognized, the events can be readily analyzed for actionable data, and Tenable's solution is easy to install and operate.

About Tenable Network Security

Tenable, headquartered in Columbia, Md., USA, is the world leader in Unified Security Monitoring. Tenable provides agent-less solutions for continuous monitoring of vulnerabilities, configurations, data leakage, log analysis and compromise detection. For more information, please visit us at http://www.tenablesecurity.com.

TENABLE Network Security, Inc.
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046
TEL: 410-872-0555
http://www.tenablesecurity.com