Organizational "Return on Investment" Using Tenable Products

April 2005
(Updated January 2009)

Table of Contents

Introduction

Tenable Network Security, Inc. is a network security software product company that offers distributed security management tools for small, medium and large enterprises. Tenable was founded by the creators of the Dragon intrusion detection systems and the Nessus Vulnerability Scanner. They provide enterprise networks a solution to efficiently manage security across hundreds of network administrators, dozens of different business units and hundreds of thousands of network devices.

Through conversations with individuals at many companies, it has been determined that their overall goals include an improvement in security posture accomplished by increased productivity and audit cycle time. It is also assumed that the Security Center will not be replacing any current security platform but will be an investment in process automation and communication improvement.

This paper describes how an organization can accomplish its goals while maintaining lower on-going costs to do so. Tenable provides this analysis and these recommendations based on several interviews with various customers and estimates gained from its experience with other similar organizations.

Return on Investment Summary

Advantages

There are several advantages to utilizing the Tenable's products, specifically Tenable's Security Center within your organization.

Automation / Increased Employee Productivity

1. Automation of mundane and time consuming tasks as it relates to scanning, discovering and organizing network vulnerabilities and intrusion events.
2. Automation of who owns the particular asset and communicating the correct remedial action.
3. Automation of both executive summaries of network risk and threat levels for executives detailed technical reports managers required to get their jobs done.
4. Increased number of cycles for auditing and remediation of your network's vulnerabilities.

Stretching Your Investment Dollar

1. Security Center allows your organization to manage events from multiple IDS sources (Snort, RealSecure, Dragon, Intrushield, Bro, NFR, NetScreen IDP).
2. Security Center allows you to leverage open-source products and even provides commercial support for the Nessus Vulnerability Scanner when it is managed by the Security Center.
3. No need to spend money on a separate database software and database administrator.

Below is an example of an organization investment in Tenable's Security Center:

Security Center / Nessus Investment (5000 IP)	Upfront Costs	On-going Costs
Active Scanner cost	$ -	$ -
Additional scanner cost (if further distributed scanning required)	$ -	$ -
Security Center Cost	$ 80,000	$ -
Annual Maintenance Cost (includes support for the Nessus Vulnerability Scanner if managed by the Security Center)	$ 16,000	$ 16,000
Database cost	$ -	$ -
IDS Correlation (supports 8 different IDS')	$ -	$ -
Fully-burdened cost of DBA to administer database	$ -	$ -
Total Investment	**$ 96,000**	**$ 16,000**

Network Security Business Problems

Managing the Vulnerability Lifecycle (Scan, Discover, Organize, Communicate recommendations, Remediate, Re-scan to verify)

Tenable can provide your company with the ability to scan all of your organizations as often as desired. Tenable utilizes the Nessus (http://www.nessus.org/) vulnerability scanner in a distributed fashion to discover systems, their services and their vulnerabilities. By using a distributed architecture, the job of scanning can be split up among several different nodes.

Improving Scan and Discovery Time

For your company, this means that your entire network space could be completely scanned for thousands of vulnerabilities each weekend. It also means that when a particular vulnerability needs to be searched for, a list of vulnerable systems can be determined within hours. By using one scanner technology across all of your organizations, a common list of the top vulnerabilities can be produced. The Security Center gives your organization the ability to conduct distributed scanning. This allows you to dedicate several scanners throughout your network so all scanning of networks can be accomplished in parallel. Below is an example of how distributed scanning allows you to scan networks in parallel and audit your entire IP range in far less time.

Scan Time Savings Estimates	Security Center - Distributed Scanning				
Number of Hosts	5,000	5,000	5,000	5,000	5,000
Number of Hosts Scanned in Parallel	15	15	15	15	15
Scan time per host time in minutes – Tenable/Nessus	6	6	6	6	6
Number of Nessus Vulnerability Scanners	1	2	3	4	5
Time in minutes to complete full scan for all hosts	2,000	1,000	667	500	400
Scan Time in Hours	33	17	11	8	7
Scan Time in Days (Assuming 8 hour work day)	4.17	2.08	1.39	1.04	0.83
Time Saved in Hours	-	16.67	22.22	25.00	26.67
Time Saved in Days (Assuming 8 hour work day)	-	2.08	2.78	3.13	3.33
Percentage improvement in speed per Nessus Vulnerability Scanner added		**200%**	**300%**	**400%**	**500%**

Organize, Communicate Recommendations, Remediate, Re-scan to Verify

The primary network security problem within many large organizations is communication. Tenable believes that information about the "security state" of a network asset should be part of a three tiered model.

- The first tier is made up of the network and system administrators who have responsibility for keeping the systems running and delivering their services.
- The second tier is the security group that is responsible for determining the vulnerabilities present on the network, their impact to the business and to track the progress made to mitigate vulnerabilities.
- The last tier is the management group that looks at the vulnerabilities and progress made by each business unit.

Security Center provides a web-based console where all users that need to scan can log in and launch scans to their assets. Once the scan is complete they can also use their account to run reports, analyze results and perform and track vulnerability remediation. Below are estimates of how the Security Center can increase the number of full network vulnerability audits and repair cycles that can be accomplished by your company.

Security Workflow - Time Savings Estimates	Security Admin & 1 Nessus Scanner	Security Center & 3 Nessus Scanners	Security Center & 5 Nessus Scanners
Number of Hosts	5,000	5,000	5,000
Number of Vulnerability Security Administrators	1	1	1
Number of System Administrators	25	25	25
Number of Hosts/Vulnerability Sec Admin	5,000	5,000	5,000
Number of Hosts/Sys Admin	200	200	200
Time to complete 1 full scan in Days (assume 8 hour work day)	4	2	1
Time to organize and communicate recommendations to sys admins	30	1	1
Time for system admins to remediate vulnerabilities	30	5	5
Time to prepare management reports	5	-	-
Total Time in Days to complete 1 full Remediation cycle	69	8	7
Percentage time improvement from automating process w/ Security Center		**89%**	**90%**
Maximum Scanning and Remediation cycles per year (360 days)	5	48	51
Percentage increase in scanning/remediation cycles per year		**920%**	**986%**

Vulnerability Remediation Articulation and Tracking

Tenable's products not only identify vulnerabilities present on your company's networks, they can facilitate a tailored conversation with each company administrator such that a prioritized view of which vulnerabilities need to be mitigated can be delivered.

Tenable's philosophy is that the relationship between IT and Security needs to be positive. We feel that any chance that a security employee has to create frivolous work for someone in IT needs to be mitigated. To combat this, Tenable has incorporated the following flexible remediation model into our products.

First, the security group can see all of the vulnerabilities and intrusions across a large network. Thanks to asset management and the scalability of Tenable's solutions, this data is prioritized and used to figure out the most critical impact to your company or each organization. The security group can also see real-time and trended intrusion detection information with Tenable's products and this may also help prioritize which vulnerabilities should be mitigated.

Second, with the cooperation of senior security managers and senior company leadership a list of vulnerabilities to mitigate can be produced. This list can be as long or as short as deemed necessary by your company.

Within each of these lists, it is up to the security group to provide mitigation information that has been localized for each component of an organization. For example, a particular vulnerability may be present on a Windows operating system, a Cisco router and an HP printer. Fixing the vulnerability is completely different on each of these network components. Also, each organization has a unique network environment. It may make more sense to firewall a device, disable it, upgrade it or a variety of other actions, rather than patch the device.

The third step in this process is to communicate this information to the administrators in each organization. Tenable's products offer a flexible method to do this. For a particular vulnerability, it is very easy to create a "recommendation". This recommendation can be communicated to only those administrators who have one or more systems or networks that contain that vulnerability. In addition, if a narrower group needs to be targeted, recommendations can be issued by vulnerability and asset type. For example, separate network management recommendations could be issued for the Cisco routers and the Nortel switches, even though they have the same vulnerability.

The fourth step is in the administrator's hands. From their point of view, they are relying on security to tell them which vulnerabilities need to be mitigated. Tenable has designed our products with the knowledge that many administrators are proactively security conscious and will not wait for a recommendation to resolve a vulnerability. To facilitate this, Tenable's products allow any administrator to see all of their raw vulnerabilities in great detail if they choose to. Some organizations even allow their administrators to conduct their own vulnerability scans with Tenable's products. However, for the entire company, the typical administrator will receive notice of only the specific vulnerabilities that have been deemed important.

As vulnerabilities are mitigated (or not mitigated) this information is communicated to senior management. By vulnerability and by business unit, such as an individual organization, the entire progress of mitigating vulnerabilities can be viewed. With Tenable's products, your company can identify and/or track which organizations have made progress mitigating their vulnerabilities. Senior company leadership can also compare this progress across different company organizations. This may assist senior IT managers to identify resource or policy lapses, or indicate that a particular technology is much more efficient at mitigating specific security holes.

Executive Reporting

Tenable's products produce a variety of reports that captures not only the trends of vulnerability and IDS activity, but also each organization's efforts to minimize their security profile. This information can allow an executive to see what their organizations are doing

with their security activity, and also capture the amount of work that they are doing per resource.

For your company, this means that each organization can be reported on individually, or all security information can be combined to produce one giant report for your company on a daily basis.

Additional Benefits to Your Company when using the Security Center to Manage the Vulnerability Life Cycle

Asset Management

Tenable believes that asset management is much more than identifying where a system is and what it is connected to, but should also include the server's owners and purpose.

Any vulnerability scanner or network management tool can provide "discovery" of network devices. However, a solution that can assign a particular device to a specific organization, a set of administrators and function is much more effective.

For example, a database of IP addresses and hardware types may be useful for inventory management, but being able to label devices such as "core network routers" or "backup human resources database" is more explicit. When analyzing security vulnerabilities or intrusion attempts, small or low-priority events on critical network resources can be identified.

Linking asset information with specific organizations and administrators also facilitates the remediation of security vulnerabilities and expedites the incident response process. Tenable has observed first hand company security personnel go through a manual exercise of first identifying which systems are vulnerable to a specific exploit, hen manually identify the owners of those systems and then to repeat this process some time later when a new high-impact vulnerability needs to be identified and mitigated. With asset management, this process is automated.

Similarly, by linking vulnerabilities, assets and intrusion data, automated incident response actions can be accomplished. With knowledge of the system's owners and asset vulnerabilities, intrusion detection events can be automatically filtered to each end user. By correlating the feed of intrusion detection events with known vulnerabilities, automated alerting of highly-critical intrusion events can also be delivered.

Although diverse systems exist throughout your company to manage network assets, Tenable has technology that can enable each organization to label each of their networks and network nodes with a unique function, place and description. Tenable's solution allows for the security group of your company or a specific organization to manage the labels in which the administrators can then apply to their systems. By controlling the types of labels available, but allowing the administrators to assign this information, a consistent view of the network can be achieved.

Security Center has a rules language that is used to assign asset types to detected systems each time a scan is run. This rules language is transparent to the user. Instead the user is presented with a simple web form that allows them to assign asset labels based on an IP address, network address, DNS name, NetBIOS name or Ethernet address. For example, if we knew that the 192.168.30.0/24 network was in New York, we could create an asset

"place" entry of New York and then create a rule that associates it with any IP address within that range. If we knew that a specific Windows NT WorkGroup of "COMPANY-HQ" consisted of Windows NT and Windows 2000 servers, we could add an asset description of "COMPANY-HQ-DOMAIN" and then create a rule to apply it.

For your company, this means that they can see vulnerabilities across their entire enterprise and then drill down by asset type. A unique vulnerability scan could produce hundreds of thousands of potential vulnerabilities. Using Tenable's solution, this data can be partitioned into more manageable business information. With slightly different report options or web interface queries, Tenable's products can quickly sort the information that applies to key routers, key servers, executive computers, corporate mail servers, human resource database servers, mainframe systems and any other types or descriptions that are needed.

Vulnerability / IDS Correlation: Leveraging legacy Intrusion Detection Systems

The type of solution that Tenable recommends for your company is to distribute their investment in intrusion detection information across all of their network administrators. Normally, large enterprises establish a specific group within their security group to monitor intrusion detection devices. This is because there is a perception that intrusion detection devices require highly skilled people and that only through looking at the aggregate of all intrusions across an enterprise can a meaningful model of intrusion activity be achieved.

Tenable believes that intrusion detection data needs to come out of the "back room" and be shared with the system administrators. This has two effects: first, it gets more people looking at the intrusion data and second, it dramatically decreases the incident response time when an attack or worm occurs.

Tenable does not want to turn every administrator into an IDS expert. However, we do want them exposed to threat information. We believe that administrators have a sense of ownership and will respond accordingly if they feel their systems are at risk or are under attack. With Tenable's products, any administrator can see the raw IDS events for their networks and hosts. They are not required to look at them, but they are available for administrators who want to be proactive. These IDS logs are also of tremendous value when conducting network troubleshooting.

For your company, Tenable can provide automatic notification of network administrators when attacks occur against vulnerable systems. This is a solution uniquely provided by Tenable. Instead of requiring an administrator to be an IDS expert, Tenable can automatically issue an alert that says not only are one or more of their systems under attack, but they are indeed vulnerable or susceptible to the attack. On a given day, an IDS system at your company may see over 100,000 attacks. These may all be real attacks and probes, but only a small percentage of these are actual system compromises or information leaks. By correlating these events with known vulnerability states of the target systems, "real" attacks can be identified.

Tenable's products can not only communicate this information to administrators, but can also send it to network management systems such as Tivoli.

Network Topology and Firewall Policy Discovery

Another aspect of Tenable's distributed vulnerability scanning is highly accurate network maps. The maps are accurate because scanning can be completed very quickly and from many vantage points.

Scans need to be completed for most organizations within a weekend. Anything longer and it will only be politically acceptable to launch scans once per quarter. Although this data is still useful, Tenable feels that up-to-date network maps are vital and that networks the size of your company routinely have daily changes.

By scanning from many vantage points, Tenable's products can identify all of the interconnections between your company's organizations and the Internet.

For example, if scanners were placed within just the data network, they may not be able to see the topology of an organization protected by a firewall and would never be able to see an organization's private connections to other organizations or 3rd party locations on the Internet. As soon as scanners are deployed within a particular organization, they can be used to identify connections to other organizations as well.

Similarly, the distributed active scanning can detect changes in firewall policies. Let us consider an example where there are two organizations that are inter-connected, but have the connection monitored by a firewall. A daily vulnerability scan from one organization to another would not find open ports on a target machine behind the firewall. However, if there was a change or lapse in the firewall policy, the ports behind the firewall would be discovered.

Lastly, not only do Tenable's products produce accurate topology maps, but this information can be viewed by anyone with a web browser. When deploying Tenable's products within your company, any administrator can see their unique network topology map. Normally, topology information is a closely held and poorly communicated piece of information. By distributing this through the network and system administrators, each person can see how their overall security and configurations may impact the entire enterprise.

Additional Products from Tenable for Your Company's Future Consideration

Passive Vulnerability Scanner

Tenable can also provide your company with the ability to passively determine their vulnerabilities with no adverse impact to the tested networks. Tenable has developed a product that can determine all of the network's vulnerabilities by analyzing the packets and sessions. It is deployed similarly to a network intrusion detection device, but only provides asset, service and vulnerability information.

For your company it is quite likely that some, if not all organizations, will object at first to being regularly scanned or having scanning occur within an organization's network. In this case, Tenable's Passive Vulnerability Scanners can be placed outside the ingress and egress points of an organization to analyze their internal servers. For example, a Passive Vulnerability Scanner placed outside of an organization's firewall would be able to identify all of the vulnerabilities in their email, web, file transfer and chat activity. A Passive Vulnerability Scanner deployed on the inside of an organization would be exposed to all of their internal traffic and would also discover more vulnerabilities.

Within the security community, it is common knowledge that active vulnerability scanning is the best way to accurately enumerate a network's components and vulnerabilities. The cost of an active scan is a negative network impact. Without extensive testing, it is difficult to

determine the impact of even a simple port scan of a large enterprise network. Network technology such as load balancers, web proxies, stateful firewalls and “application aware” switches do not behave well when presented with numerous vulnerability scans. Tenable stands behind conducting active vulnerability scans, but also offers passive vulnerability scanning as an alternative or supplement to Scientific Atlanta, and also as a way to minimize the number of active scans required to monitor your company’s organizations.

Log Analysis with the Log Correlation Engine

Tenable recognizes that log analysis for security events is a vital part of any network security program. Current solutions in this space are highly complex, expensive and require highly trained staff. Tenable has introduced the Log Correlation Engine which allows the Security Center to analyze firewall logs, IDS events, server logs, application logs and proprietary devices.

There are many types of network devices that produce log events. There is no way to predict what all of these log formats look like or if they will change in the future, which makes common analysis very difficult. For example, it would be desirable to correlate Apache web logs with Checkpoint firewall logs, but they are in different formats. To help with this, Tenable has developed a method to use high-speed plugins to parse logs from many different sources into a normalized format. The Log Correlation Engine currently supports more than 100 different event log sources and the plugin language is incredibly easy to extend to new devices. As the Log Correlation Engine reads the event stream, it assigns a normalized name to each matching plugin. An Apache web login failure could be reported as an “Apache 404 Logon Failure” event and a blocked TCP connection at a Cisco PIX firewall could be reported as a “Cisco PIX TCP Deny” event. Both events would have the relevant IP addresses, ports and protocols labeled inside the Log Correlation Engine’s data schema for events.

Tenable has developed a process for automatically detecting trends and deviations from “normal” network activity. 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. Alerts can be generated if there are any fluctuations in these “normal” loads. Events that are only slightly statistically significant can be used as pointers to understand “normal” network behavior. This is very important concept because network usage, load and communication flows often change on a daily basis.

Tenable has produced the Tenable Application Scripting Language (TASL), which is similar to 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.

All of this analytical power can be used to extend any Security Center. Users of the Security Center have particular ranges of IP addresses for which they can see vulnerabilities and intrusion events. With the Log Correlation Engine, this still holds true. This means that a Security Center user who can only see events associated with their specific servers will only see logs for their specific servers as well. For example, a Security Center user who is an administrator for 10 DNS servers would be able to see the firewall logs that impacted one or more of their systems.

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/