TENABLE
Network Security®

Network Security Implications of “Visible Ops”

February 7, 2007
(Revision 7)

Table of Contents

Introduction

This paper will examine how Tenable's converging set of vulnerability management, security event management, and compliance reporting tools interact with common network management practices known as "Visible Ops". After reading this paper, readers will have a basic knowledge of network management theory and how Tenable's products can help manage networks efficiently.

What is "Visible Ops"?

Simply put, "Visible Ops" is a handbook written by Gene Kim and Kevin Behr which summarizes network management theory known as "ITIL". The handbook helps classify the type of network management which exists, and defines how organizations can move from less efficient to more efficient operations. The handbook is loaded with "common sense" arguments for better forms of network management, likely counter-arguments to these more efficient management forms, and multiple ways to measure progress and increases in efficiency.

According to the handbook, there are four stages of network management. These involve establishing change control, determining the most fragile network components, establishing a "repeatable build" process, and finally, measuring the effects of each of these processes by tracking statistics on available uptime, average time to recover from an outage and number of successful changes.

At each of these phases, how to measure success and failure in terms of resources gained as well as management support is established.

The "Visible Ops" methodology allows for the identification of network organizations which are either a "high performer" or "inefficient". This is simply the measure of uptime, server to administrator ratios, change success rates, and other parameters. A trend discussed in "Visible Ops" is that most "high performer" networks have higher server to administrator ratios, less overall change, and little variance in the configuration of their servers. We will examine many of these concepts throughout this paper.

Inefficient IT and Security Groups

What does it mean to be inefficient for IT?

There are definitely two types of networks. Those that have high availability rates and those that do not. Typically, those that have high availability rates have a higher server to administrator ratio and less deviation in the servers they manage than other groups. A less efficient group will have lower uptime for their servers and a large percentage of their time consumed by unplanned outages.

There have been statistics gathered which show that 80% of all outages are self inflicted. Applying simple change management control immediately returns a large number of man-hours as well as infusing confidence into the network users and administrators.

What does it mean to be inefficient for Security?

For a security group, efficiency should be measured by how quickly risks can be determined and how quickly incidents can be responded to. Unfortunately, most security groups do not look at themselves this way and tend to think of themselves as a necessary evil.

Infrequent Security Profiling

For example, consider vulnerability scanning. The function of the scan is to find existing or new vulnerabilities. The best time to find a new vulnerability is before it gets added to the network. If security has no visibility into what IT is doing, it is crippled by taking snapshots from monthly or quarterly scans. This elongates the process of discovering and eventually removing any vulnerabilities.

There are many reasons for the limitations in scanning. In some cases, the actual scan has caused an outage in an application, server or network node. In some cases, there is political opposition to the scanning. There may also be physical limitations to how fast a scan can be completed.

Because of these limitations, the security group only obtains a glimpse of the true nature or profile of the IT group.

There are two very important issues with this to consider. First, security changes the ruler they use each time they scan. For example, the list of vulnerabilities “checked for” is always growing. This means that even if an IT group were to patch everything as fast as security could tell them, they still may be full of security holes. Without accurate change management, an unprepared IT staff will always be “fixing” vulnerabilities in their network. Although this sounds like a positive thing, what actually will be happening is that the team will be creating large amounts of variance in their infrastructure. This large amount of change will increase operational costs.

Second, infrequent scans show little visibility into actually how well IT is managing their servers. For example, what is their “mean time” between failures or their time to recover from an outage? Many high performing network organizations suffer security outages the same way they deal with power, personnel, and traffic utilization issues – they build redundancy and scalable solutions and procedures.

The theme of these last two points is that IT has little chance of passing a security audit, even though it may be the most efficient organization in existence.

Random Incident Response

There is a similar ad hoc model for incident response. Since no one can control when an incident occurs, the assumption is that the security group will discover the event. What happens in practice though is that it is IT that notices a deviation from normal server or user behavior. This may come from an odd user complaint to a help desk, from the loss of connectivity to the Internet or some other alarming condition.

There have been many studies that recognize the fact that a majority of all incidents occur internally by malicious or misguided users and not external forces. However, most security groups preach a defense in depth strategy and tend to look outward for signs of an incident.

Politically, when IT does discover an insider threat, it gets handed to the security group for intervention or monitoring. However, when this occurs, security does not usually have access to the configuration of the systems under investigation, or the configuration of the supporting systems around this. IT may be able to provide some of this information.

Discovering Who is Responsible

Inefficient IT and security groups tend to expend considerable amounts of time discovering who owns a system or even where it is located. For a stereotypical example, once a security group completes a scan, it may have 100,000 vulnerabilities discovered for 20,000 unique IP addresses. Unless IT has a very good asset model on where these devices are and who owns them, there is little chance that these vulnerabilities can be fixed.

This is extremely important because the model viewed by many people in security is 100% remediation of every vulnerability. For an operating system, this means applying a patch which to IT means extra work and potential downtime.

However, taking a holistic view, if IT (and security) had a very good list of which servers and systems were "important", the task becomes less daunting. Knowing where an organization is exposed the "most" is critical to being efficient.

Similarly, knowing what these server functions are can help imply the fix. Three routers may have the same easily guessable SNMP public string, but the process to remediate the wireless router, the office router, and the core gigabit router should be different. This is because any change made to a device can impact other systems. The gigabit router is likely supporting thousands of users and services. The wireless router may also be linking critical remote services. The point is, knowing what a fix may break or impact is just as important in some cases as applying the fix. Applying security fixes blindly creates unanticipated outages and reduces efficiency.

Similarly, all vulnerabilities are not remediated the same way. With the same SNMP example, a printer, a Windows 2000 server, and a router may all have the same vulnerability, but the steps to mitigate it are vastly different. If the security group is telling the folks in IT who manage the routers to change their Window's registry settings (there are no registry settings on routers), this also reduces efficiency by wasting time for both the IT and security groups. If security had better visibility into what was on the network, they could be more accurate in recommending security fixes.

Tenable Solutions and the "Visible Ops" Handbook

Increasing Efficiency

Tenable Network Security uses the concepts of "Visible Ops" to assess how mature our customer's network management processes are. This allows us to bring the greatest benefits of our products to assist the customer in moving to a more efficient network management state.

Although simplistic, Tenable can classify customers into four broad categories:

- Lack of pervasive change management
- Effective change management, but lack of common build processes
- Common build processes, but lack of end to end measurement of IT metrics
- Improvement and reporting on the overall IT process

For each of these states, Tenable's solutions can help limit the overall security exposure as well as help in transcending to the next state. In the terminology of "Visible Ops", network managers are encouraged to take their network resources and staff through the following process:

- Stabilize the patient
- Find fragile artifacts
- Establish a common build library
- Continuous improvement

We will briefly discus each of these phases and the impact of Tenable's solutions within that phase.

Stabilize the Patient

When moving the network from a lack of network change management to one with change control, the absolute first thing to do is to stop making undocumented and unauthorized changes. This is known as "stabilizing the patient". By freezing change, network managers can limit the outages caused by unexpected changes.

For security practitioners, attempting to limit the amount of vulnerabilities in such an uncontrolled network or detect and respond to intrusions is a daunting task. Because there is so much "unknown", any type of automation can assist the security practitioner. Also, for larger networks, the volume of what is "unknown" can be difficult to comprehend. Fortunately, Tenable's solutions can assist large and small networks to get a handle on network security while the patient is being "stabilized".

Tenable has several products which perform vulnerability scanning, vulnerability traffic monitoring and host-based security assessments. These allow any organization to quickly discover what is on their network and which vulnerabilities are the most critical.

By using a combination of scalable active, passive and host-based technologies, security groups can provision Tenable's solutions to sample the state of network security in extremely large volumes and much more often.

For example, many people are familiar with the concept of a vulnerability scan. From Tenable's experience though, most network security practitioners are not proactive enough and scan infrequently. This makes it extremely difficult to detect change and trends from vulnerability scans. With Tenable's solutions, multiple scanners, network monitors, and host-based analysis tools can be used to sample the network in real-time with complete audits. This allows for subtle change detection of the network and its applications.

If scanning is not an option, Tenable also has products which "sniff" network traffic and produce the same (if not more accurate) list of vulnerabilities. This occurs in real-time and has no network impact. If a server or application communicates on the network, it will be discovered without the requirement of a vulnerability scan.

The combination of active and passive monitoring for vulnerabilities also has natural change detection. New hosts, new applications and even firewall rule changes can be detected this way. If they are occurring outside of known change management windows, this can be of great assistance to the network managers who are trying to implement proactive change management procedures. Tenable's solutions can report on any type of vulnerability, including new hosts and applications for specific asset classes. For example, this could allow a network manager to compare the effectiveness of change management procedures between two different data centers.

Lastly, Tenable's solutions also enhance the incident response process. Tenable has solutions which aggregate intrusion and log information and instantly correlate it with existing asset and vulnerability information. This allows an effective incident response capability to be developed, even when absolute change control and network management processes have not been in place yet. Tenable's solutions can be leveraged not just by the security group, but by the application, server and network administrators. When an incident occurs, the actual system owners can be targeted for direct alerting.

Find Fragile Artifacts

Once a change control process is in place, the next phase outlined by "Visible Ops" is to discover which systems are the most critical. These systems may be deemed important because they are the most likely to have an outage, because they have large numbers of changes made to them, or because there are many other systems dependant on them. Tenable's solutions can assist in the discovery of these systems.

First, of the three forms of vulnerability discovery technologies that Tenable produces, the most potentially destructive to a network is the vulnerability scan. The other two technologies, passive network monitoring and host based auditing, have almost no system or network impact. However, since network scanning tends to exercise applications and protocol implementations in ways they were not intended to perform, the possibility of outages in network gear or applications can occur. In addition, Tenable's vulnerability scanners come pre-loaded with a variety of vicious "denial of service" tests which are disabled by default, but can be used to test just how solid a server really is.

Second, Tenable's vulnerability management tools allow multiple types of asset designators to be overlaid onto the existing vulnerabilities. This allows a large volume of vulnerabilities to be more easily analyzed for the true impact to the network or specific asset classes. For a simple example, consider a medium network with one web server that has a medium vulnerability and one hundred desktops all with medium vulnerabilities in their web browsers. A report would show one hundred and one medium vulnerabilities, but the most critical vulnerability would be to fix the single web server. With Tenable's solutions, the most "interesting" asset classes can quickly be analyzed to find out their unique vulnerabilities.

Lastly, when discovering where these fragile artifacts are, it is important to know what systems communicate with them. For example, a web application may make queries to a database server. If the web application was scanned and found to not have any vulnerabilities, but the database server had many vulnerabilities, a fragile artifact may not be identified. With Tenable's passive monitoring technology, trust relationships can be discovered between specific servers and asset classes. This allows dependencies to be understood and the vulnerabilities on one dependent system to be projected onto other systems as well. This technique also works in reverse such that a secure server being administered by an insecure client can also be identified.

Establish a Common Build Library

Once change control has been implemented and the critical assets identified, the next phase prescribed by "Visible Ops" is to start building things as uniformly as possible.

One of the key themes within “Visible Ops” is to reduce the amount of variance among systems. This reduces the amount of guesswork in maintaining a system and increases the effectiveness of change management. For example, when patching several hundred servers, often a certain number of the patches fail due to conflicting software. If these servers were more uniformly configured, there would be a higher number of successful changes.

The most effective way to ensure that systems have a lack of variance is to enforce this as they are added to the network. By implementing a common and repeatable build process, all new desktops and servers can be guaranteed to have a certain level common configuration. It may seem counterintuitive to re-install an operating system on a brand new server or laptop, but without doing that, there is no way to know for sure that there is unauthorized software or configuration settings on these systems.

Tenable’s solutions offer two strategies to help enforce and detect when a process to implement similarly configured systems is in place. These both involve using vulnerability scanning of systems in place and prior to being added to the network.

First, the vulnerability information collected can be used to search for “variance”. This involves searching for similar types of systems with different configurations. Regardless if configuration information is obtained through scanning, passive network monitoring, or host-based analysis, Tenable’s solutions can compare different asset classes of devices for many types of configurations including:

- Open ports
- Windows Registry Settings and Unix configuration files
- Client and server software versions
- Missing operating system patches
- Presence of spyware, Trojans, and backdoors

For example, with these parameters, a user of Tenable’s products could produce a listing of all “web servers” and then compare what ports they had open. We would expect that there would be port “80” or possibly port “443” which is used for encrypted sessions. However, if ports for FTP, email, chat, or other protocols started to show up, this could indicate variance.

Since Tenable’s solutions can be configured to conduct periodic scanning and continuous network monitoring and the results be used securely by non-security staff, anyone in IT can search the network for variance anytime they need to investigate an issue or generate a report.

Second, prior to a server or desktop being added to the network, a vulnerability scanner is an excellent way to collect baseline information about the configuration of a system. Besides simply auditing network services, Tenable’s vulnerability scanners can be configured to make use of Unix or Windows credentials to audit any type of internal configuration setting. These scans can be saved as a catalog of templates, for a repeatable test, depending on the type of asset.

For example, a corporate desktop might be configured to be part of a specific Windows “domain” and have the desktop firewall enabled. A vulnerability scan could “prove” that a machine was configured this way at one point. Processes can be put in place not to let any machine be added to the network which did not pass their vulnerability scan.

Continuous Improvement

The last stage of network management as outlined by "Visible Ops" is simply to put the previous three steps into more and more levels of efficiency. No network management system is perfect, but by conducting after-action investigations to find the root cause of outages and lapses in procedure, continuous improvement can be afforded. With network management in place, and generally high availability times for network servers, many organizations track the following statistics:

- Availability – the overall percentage of time the system is available
- Mean Time to Recover – the average amount of time it takes recover an outage
- Change Success Rate –percentage of time that changes made to a system succeed
- Server to Admin Ratio – number of servers divided by number of administrators

Of course the largest statistic most organizations track when it comes to operating a network is the complete cost of running a network. If each of the above statistics is improved, there will be a subsequent reduction in network costs. For example, an increase in the "Change Success Rate" may imply that less administrators will be need to complete change across the entire network.

Also, each of these statistics may not mean much by themselves, but when trended across both time and against other organizations, they are much more useful. For example, a server with an uptime of "90%" may seem impressive, but knowing that it was at "95%" for the previous ten weeks could indicate an issue. But if we knew that through the rest of the organization, uptimes of "85%" were more common, we would still consider this network to be a high performer and not a problem.

With Tenable's products, the same approach can be taken with measuring security metrics. Tenable's products allow many organizations to have their vulnerabilities and security events measured often and compared to each other. For example, one of Tenable's unique management reports is a simple two page executive summary of all vulnerabilities and intrusion events for the past ninety days, followed by a graph of all security work-flow events and security resources.

At a glance, senior management can see actual trends in security for any organization, or even use this data to compare one organization with another. This allows for management to have the proper context when dealing with security issues. Too often security delivers a message of "dramatic consequences" unless immediately addressed. This creates the "sky is falling" type of fire drills that senior managers do not like to deal with. By placing each business unit on its own and comparing their trends with vulnerability management and incident response rates over time, managers can easily see which groups need attention and which do not.

Conclusion

As network management and control matures by using the "Visible Ops" approach, Tenable's product offerings can be used to assist in the detection and management of all security issues. Within each phase, Tenable's offerings help organizations overcome a variety of technical and political hurdles when attempting to sample the true state of security for a given network.

About the Author

Ron Gula is a Founder and Chief Technology Officer of Tenable Network Security. Tenable is a company that produces the Lightning Proxy for high-speed Nessus vulnerability scans and the Security Center for correlating IDS data with Vulnerability data and making it available to multiple people in multiple organizations. Previously, Mr. Gula was the original author of the Dragon IDS and CTO of Network Security Wizards which was acquired by Enterasys Networks. At Enterasys, Mr. Gula was Vice President of IDS Products and worked with many top financial, government, security service providers and commercial companies to help deploy and monitor large IDS installations. Mr. Gula was also the Director of Risk Mitigation for US Internetworking and was responsible for intrusion detection and vulnerability detection for one of the first application service providers. Mr. Gula worked for BBN and GTE Internetworking where he conducted security assessments as a consultant, helped to develop one of the first commercial network honeypots and helped develop security policies for large carrier-class networks. Mr. Gula began his career in information security while working at the National Security Agency conducting penetration tests of government networks and performing advanced vulnerability research.

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