Interested in learning more about security?

SANS Institute InfoSec Reading Room

Strategies for Improving Vulnerability Assessment Effectiveness in Large Organizations

Implementing or maintaining a vulnerability assessment program in a large organization requires a dedicated team to conduct the assessments, and to evaluate the findings. In most businesses, security is not a revenue generator; indeed, it is a cost center. In order to provide value, you must either improve the effectiveness of the program, or reduce the drain on resources. There are several steps that can be taken to reduce the impact to your environment, to include: effective communication of the program, use of appro...

Robert Huber
Version 1.4b (amended August 29, 2002)
GSEC Option 1
April 20, 2003

Strategies for Improving Vulnerability Assessment Effectiveness in Large Organizations

Table of Contents

Abstract

Implementing or maintaining a vulnerability assessment program in a large organization requires a dedicated team to conduct the assessments, and to evaluate the findings. In most businesses, security is not a revenue generator; indeed, it is a cost center. In order to provide value, you must either improve the effectiveness of the program, or reduce the drain on resources. There are several steps that can be taken to reduce the impact to your environment, to include: effective communication of the program, use of appropriate change and enterprise management, placement of assessment tools, tuning the assessment policy and automating the assessment. In addition, a new process to manage the assessment data, termed vulnerability management, has materialized. This spawned the creation of several new solutions to address the issue of data management. Combined with the essential elements stated above, these tools will increase the effectiveness of your vulnerability assessment program.

Strategies for Improving Vulnerability Assessment Effectiveness in Large Organizations

Introduction

In large organizations, vulnerability assessment places a tremendous strain on available resources, both information technology, and human. Vulnerability assessment is a necessary evil, to reduce the risk against the confidentiality, integrity and availability of information technology assets. In order to provide the most value to the organization, the benefits of the vulnerability assessment program must outweigh the risk of doing nothing, or some combination thereof. When determining how to implement a vulnerability assessment program, you must understand the impact of operating the program itself to reduce the impact to the environment from both an information technology and human resource perspective. In addition, you must be able to show a full lifecycle of risk management which provides the relevant metrics to senior management that the risk is actually being reduced.

This paper will detail how to reduce the impact of the vulnerability assessment program in your organization, how to provide actionable items to those responsible for performing the work, how to effectively reduce high risk, and how to provide senior management with metrics that show actual risk reduction. In addition, this paper will review three vulnerability management tools which are aimed at presenting a full lifecycle risk management approach and how they can aid in increasing effectiveness and your return on investment.

Reducing the Impact to the Environment

If the benefit of a vulnerability assessment program is to reduce risk, then the reciprocal, to not increase risk, is also true. As dumb as that may sound, many are surprised to find out that improperly communicated, improperly configured and improperly executed vulnerability assessment programs can have an extremely negative impact on their environments. This can vastly affect the service level agreements of the organization, most notably, availability. In turn, this affects the overall benefit of the vulnerability assessment program in terms of cost and resources. To improve the chance of success for the vulnerability assessment program, several items must be considered: communication of the program, use of appropriate change management, placement of network assessment tools, and diligence in defining the assessment policies.

Communication of the program

To aid in the success of the vulnerability assessment program, it must first be communicated to all levels of the organization. This starts at the top and works its way down and usually takes the form of policies, standards, guidelines and procedures, with policies being more general in nature and procedures more specific (Krutz and Vines 11-12). In order to gain understanding and permeation, security awareness must take place from the senior management level down to the system administrator. This includes addressing the scope of the program,

the frequency, execution and the potential impacts to the environment, as well as the benefits. It is important to note during the awareness campaign any regulatory or legal requirements for operating the program, such as the Health Insurance Portability and Accountability Act (HIPAA), the Graham-Leach-Blilely Act (GLBA) or regulations from the Office of the Comptroller of the Currency (OCC). There are numerous articles written on security awareness available in the Sans Reading Room, http://www.sans.org/rr/aware/ .

Use Appropriate Change and Enterprise Management

Most large enterprises have a structured change management process in place. Change management allows for the tracking of changes to the information technology environment and the communication of impact to any affected parties. Once you have determined asset owners, and a schedule to perform the vulnerability assessment against those assets, the change management system must be utilized to alert asset owners. This establishes an agreed upon window of time to analyze the assets, and provides the owners with the information regarding your activity, as well as appropriate contact information should an issue occur. The change management system then doubles as a way to provide metrics regarding the success or failure of your assessment. In addition to the change management system, should issues arise, be sure to utilize your enterprise management system to record outages, impacts etc... Both facilities provide a lessons learned log of your activities should there be a negative impact. In addition, they create a level of comfort with the device owners, and provide accountability for your actions.

Placement of Network Assessment Tools

Deploying vulnerability assessment across a large enterprise requires careful consideration so as not to increase the impact of your assessment. Most vulnerability assessment tools were intended for the lone security consultant to come and assess your network from one laptop, then return days later with the analysis. In large organizations this will not suffice. Using one device to cover thousands of nodes across multiple classes of networks will cause more harm than good. The more touch points between you and the target, the more there is a chance of something going wrong. In this case, touch points could be switches, routers, proxy devices, load balancers and firewalls. Any one of these components can fail thereby affecting the availability of the environment. Ideally, you want to place a scanner in every network where you want to scan; however, this is not feasible in practice due to cost constraints.

For high risk areas, such as demilitarized zones (DMZs), it is advisable to deploy scanners within that segment of the network. This reduces the burden on the firewall, and increases the security of the assessment process by not requiring allow all rules on the firewall itself. For other areas, such as server farms, scanners can be deployed one per geographic location. This alleviates the impact of scanning across network circuits and localizes any issues to the site the activity is actually occurring at. According to Ron Gula, CTO of Tenable

Network , "By placing the scanning agents closer to their target networks, the port scans and other probes don't flow across the core router and switching fabric. This causes less network outages and performance degradation [. . .] " (Gula 8) . This is the concept of distributed scanning.

Distributed scanning has many advantages as identified in Ron Gula's whitepaper, Dedicated and Distributed Vulnerability Management, "By distributing the scan across many nodes, parallel scanning can occur [. . .] splitting up the effort can greatly reduce the time it takes to scan a network " (8). This also allows the organization to quickly assess the risk posture of the network if a new flaw is discovered. A perfect example would be the recent Slammer worm. In order to quickly assess a large organization, distributed scanners were a must to reduce the time and burden to complete the scan and provide the organization a quick understanding of their exposure.

Tuning the Vulnerability Assessment Policy

Many assessment tools are very powerful and can wreak havoc on your network and assets. This necessitates the need to refine your policies to only look for vulnerabilities which are relevant to your network, and which will not cause outages when they are executed. This may mean turning off denial of services (DoS) attacks, or attacks which are likely to cause a server outage. Some scanners such as Nessus will tell you if the attack has a high probability of causing an outage. According to Information Security magazine's recent testing, "Although most of the configuration [vulnerability] tools have options to disable 'dangerous' or 'denial-of-service' scanning, that isn't always sufficient to keep them up" (Snyder). If you feel it is absolutely necessary to test your devices against these attacks then I suggest you perform them in a closed test environment.

In addition to tuning your policy to remove DoS attacks and those that may cause an outage, it is also suggested that you run platform specific policies against corresponding assets. This means creating a Windows 2000 Internet Information Server (IIS) web policy and running it against corresponding assets. This increases the efficiency of your assessment time, and alleviates unnecessary network load. Obviously there is a balance which must be struck. You do not want to create a policy for every combination of assets and software you have, but a few generic groupings by operating system, as well as some that correlate to DMZ areas should be considered.

Automating the Assessment

The next step is to setup the schedule for the assessments. Based on your environment, and the criticality of the assets, you need to establish a recurring assessment schedule. I have combed through dozens of documents on best practice vulnerability assessment; nonetheless, I could not find any substantial identification of timeframes for conducting assessments. Obviously, you should frequent your higher risk areas more often. Even so, once you identify the

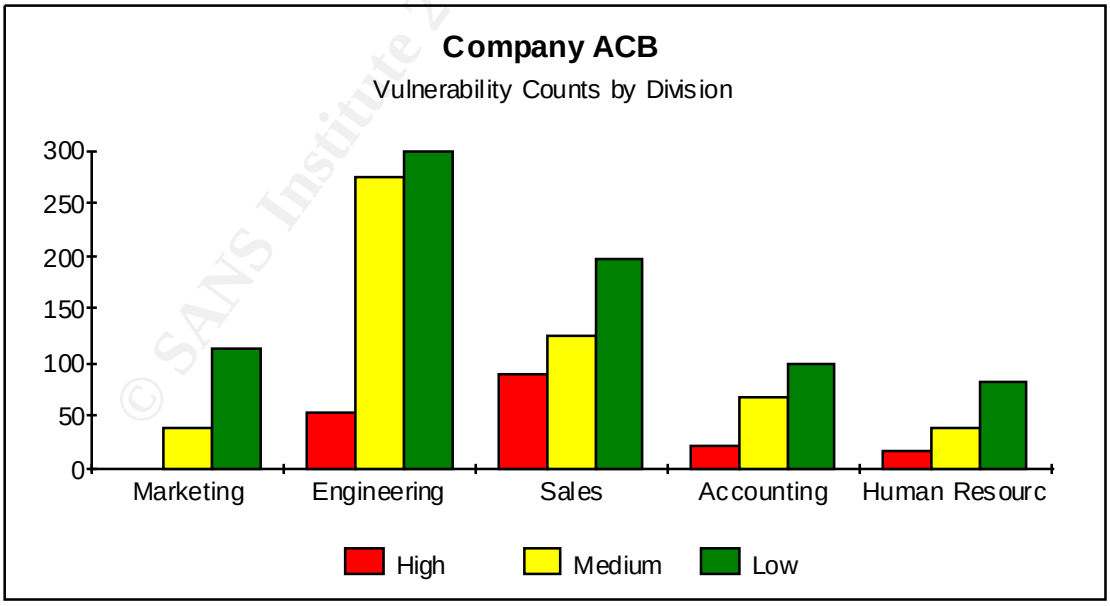
timeframes, daily, weekly, monthly, quarterly, make them part of an established schedule and make sure this schedule is communicated to those groups impacted. Ideally, your tool should include the ability to schedule assessments within time windows. If the scan does not complete within the window, then the assessment will stop. That alleviates you from impacting the devices outside of your assessment window. Automated assessment also reduces the burden on your staff and allows them to focus on the mitigation of risk, the tuning of policies and the management of the infrastructure itself.

Remediation Management of Vulnerability Assessment Data

Once you communicated the program, deployed your assessment tools, tuned your policies and began executing your assessments with appropriate change management, you will quickly start amassing data that you must now understand, prioritize and mitigate.

Reporting and Analyzing the Vulnerabilities

In a large network the number of vulnerabilities discovered can be staggering. This creates data overload for the vulnerability analyst and a nightmare for reporting. Many tools provide several views for the assessment data to include: reports by IP address or host, reports by vulnerability, reports by severity and reports by subnet. Each of these reports has an intended audience. It is essential that you get the correct reports to the intended audience to ensure that the audience can take appropriate action. Obviously, the chief technology officer does not want to see a report by IP address, host or vulnerability. The CTO looks at security from an enterprise perspective, such as a division, or line of business. As in the example below.



This creates actionable data and provides focus from a senior management level which can then be passed down to the next level. At each level your report gains more detailed information pertinent to that area which then becomes actionable.

Unfortunately, in a recent Information Security magazine review of five vulnerability assessment tools, Joel Snyder stated that "none of the five test products stood out for their data management capabilities". This will impair the end users when they are trying to drill down through their data.

Weighing the Risk

At this point you have given a report to all levels of the organization which details the vulnerabilities identified. Although this provides a starting point for action, it does not help you decide which vulnerabilities should be addressed first. To help you do this, you should have an asset inventory that details each device on your network and a corresponding rating for the confidentiality (C), integrity (I) and availability (A) for that device. As noted by Al Berg in Information Security Magazine, "Identify the business exposure of each technology on your network. Think about the impact on your business if each of these elements was compromised or made unavailable" (Berg). Once you have classified your assets, you can use the values to perform a risk analysis, such as the process identified in The CISSP Prep Guide. Below you can see elements of this process and walk through a few examples.

Since it is difficult at best to assign a monetary asset value to a device in your organization, you can substitute the calculation of C x A x I to determine the asset value. You can then use this asset value multiplied by the exposure factor, which equates to the severity of the vulnerability, to calculate a risk level, or single loss expectancy. You can carry that calculation a step further by multiplying the single loss expectancy value by the annualized rate of occurrence (ARO) which yields the annual loss expectancy (ALE). The ARO is a value that identifies the frequency with which a threat may occur. This may increase or decrease with respect to where the device is located, such as in a DMZ, or the ease of executing the exploit, or the availability of the exploit in the wild. (Krutz and Vines 16-19)

$$SingleLoss\ Expectancy\ (SLE) = AssetValue\ (AV) \times ExposureFa\ ctor\ (Severity)$$

$$Annualized\ LossExpect\ ancy\ (ALE) = SLE \times Annualized\ RateofOccu\ rrence\ (ARO)$$

Here are some scenarios that put these formulas to use. For an asset in your data warehouse housing customer data, used for weekly reporting, the C, I, and A ratings are 3, 3, and 2 respectively on a scale of 1 to 3, with 3 being the highest rating. Assuming you have a vulnerability with a severity rating of 3, and an ARO of 1 the calculations would be as follows:

$$AV = 3 \times 3 \times 2 = 18$$

$$SLE = 18 \times 3 = 54$$

$$ALE = 54 \times 1 = 54$$

Compare this to a print server with C, I, and A ratings of 1, 1, and 2 and a vulnerability with a severity rating of 3 and an ARO of 1 as calculated below.

$$AV = 1 \times 1 \times 2 = 2$$

$$SLE = 2 \times 3 = 6$$

$$ALE = 6 \times 1 = 6$$

You can see how the device in the data warehouse has a higher ALE, as you would expect. To see how the ARO affects the value, compare the above examples to a web server located in a DMZ with C, I, A rating of 1, 3, 3 and severity rating of 3 and an ARO of 3 you get:

$$AV = 1 \times 3 \times 3 = 9$$

$$SLE = 9 \times 3 = 27$$

$$ALE = 27 \times 3 = 81$$

From the calculations performed above, it becomes evident that the device in the DMZ has a higher ALE that the other internal devices, even though all three devices have a high severity vulnerability. Armed with that information, the DMZ device should be your first area of concern.

Assigning Ownership

Once the vulnerabilities are identified and risk rated, they are then ready for distribution to those responsible for mitigating the risk. Providing a report of the vulnerabilities raises awareness and gives the system administrator a starting point; however, it does not assign ownership. To assign ownership there must be two items in place. First, is a policy or standard that identifies a process for mitigation. This policy should outline the roles and responsibilities for all parties involved. This creates the ownership necessary to enforce compliance. Second, a tool, or process to track the ownership is mandatory. This provides evidence of the accountability, and can be reported to management.

Resolving the Issues

A tell tale statement by Foundstone CEO George Kurtz captured by Illena Armstrong in SC Magazine states "The finding of the issues is half the equation - the other half is getting them fixed" (qtd. in Armstrong http://www.scmagazine.com/scmagazine/2003_01/feature_1/). If you have hundreds of high risk vulnerabilities in your organization, you obviously cannot address all of them immediately. This is where the value of weighing risk becomes evident. It provides a means to allow you to focus on the assets with the highest risk first and provides a focus for the system administrator. One must also be capable of tracking the status of a vulnerability from the opening, to the closing of the issue. This allows for progress to be measured, and items to be removed from the queue as they are mitigated. Providing the ability for the end user to insert comments regarding progress is also essential. The comment section can later be used to compare similar issues in the future, as well as an area to document compensating controls, or identify other reasons for the issue remaining open.

Keep in mind that all fixes must be channeled through your organization's change management process, "when reports [. . .] recommend certain

modifications to a system, the company should have a 'change management process' in place that helps to assign duties, track their progress, inform on their effects, note their completion and more [. . .]" (Armstrong http://www.scmagazine.com/scmagazine/2003_02/feature_2/).

Verification

The last important piece of the vulnerability management process is to verify that a risk has actually been mitigated. Ideally the end user should be able to perform the verification scan against the specific issue, and once it is confirmed, then it can be passed to the security team for further verification and closure. Tools such as Nessus allow you to run a differences report against the previous scan to determine any changes, such as issues being mitigated. A report of the mitigated items is the real value that you provide to management. This lets them know exactly what issues have been addressed, and what progress has been made. These reports can then be used to calculate a return on investment when compared to potential losses.

Gaps

All of the above mentioned facets of vulnerability management are ideal requirements for any tool selection you may be contemplating. Unfortunately, most tools do not allow for varying levels of reports, from executives to system administrators. Nor do most of them allow you to weigh the risk by confidentiality, integrity or availability of the asset. Most do not allow you to track the ownership. Add to that, most tools do not allow you to follow the remediation lifecycle process to closure. Most organizations end up building homegrown solutions to address many of these shortcomings. This development effort detracts from the real mission of managing risk; hence, a new revolution of vulnerability management solutions gives rise.

New Breed of Tools that assist in Full Lifecycle Vulnerability Management

Concept

These new solutions lay aside the term of vulnerability assessment, and replace assessment with a term that implies more of a process, management. Also, the new solutions give way to enterprise wide scale, alas the fact that a single scanner is no longer sufficient for a large organization. In addition, these tools focus on the management of risk, that is, the identification, the weighing of risk, assigning ownership, tracking issues to closure and verifying the changes. Let's take a look at three of these solutions: 1). Latis StillSecure VAM, 2). Foundstone Enterprise, and 3). Tenable Network Security Lightning.

Latis Networks StillSecure™ Vulnerability Assessment and Management Products

As the name implies, Latis has taken a risk lifecycle management approach. As stated in their literature, "The VAM family of Vulnerability Assessment and Management products identify, track, and manage the repair of vulnerabilities . .

." In addition, their technology, called Vulnerability Repair Workflow, "…manages the remediation process through repair verification" (Latis, http://www.latis.com/products/svam/vam1.html). For this discussion, we will focus on their network product, called Server VAM.

Strengths

Server VAM can be deployed across an enterprise to reduce network burden and increase the efficiency of the assessment. Server VAM also has the ability to tune the assessment policy on the fly to "maximize scanning efficiency and reduce the burden on your IT staff" (Latis, http://www.latis.com/docs/StillSecure_VAM_family.pdf). VAM provides the ability to track device profiles, which includes assigning a level of importance. The importance level will then be used to prioritize the issues. As new vulnerabilities are identified, VAM automatically assigns them to the responsible individuals, and prioritizes them based on the device's impact. The end result is the creation of a repair schedule based on prioritized risk. When a user reports that an issue has been mitigated, VAM will run a verification scan to ensure it. This can be done by the end user, or in the next assessment cycle. In addition, the most critical piece, VAM has the capability to track vulnerabilities to closure as evidenced in the screenshot below.

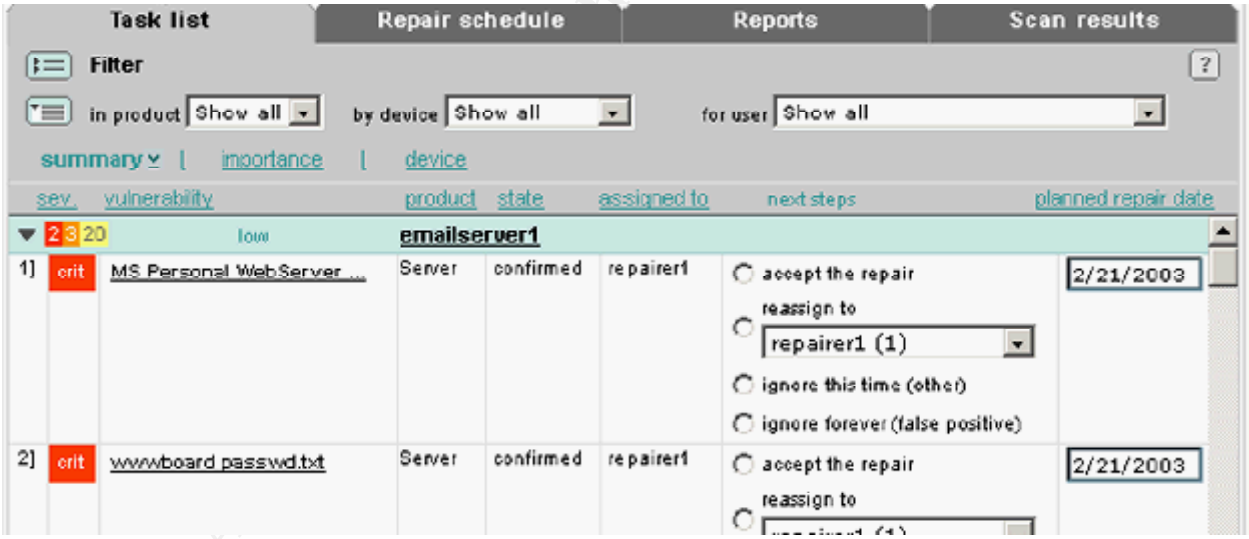


Figure 1 Latis Networks StillSecure™ VAM Task List
http://www.latis.com/products/svam/vam_server.html

Areas for Improvement

The only weakness found was the use of assessment windows. If you define a window to perform your assessment in, VAM will not stop once you have exceeded the window. This makes it difficult to ensure the asset owner that your assessments are only run during defined periods.

Foundstone Enterprise™

Foundstone recently introduced the enterprise version of its own managed service assessment solution. Foundstone Enterprise™ makes it known upfront that it is a tool to mitigate risk. An excellent quote from Foundstone regarding vulnerability assessment tools and risk mitigation is, "Vulnerability assessment tools help but don't address the real problem. Rather than simplifying security, current vulnerability assessment tools flood users with reports that include vulnerabilities of varying severity and ignore important distinctions in asset criticality". (Foundstone http://www.foundstone.com/products/index_products.htm). Foundstone Enterprise has three components: the Foundscan Engine™, Foundstone Enterprise Manager, and Foundstone Security Factors™. The engine is the network scanner itself. Foundstone Enterprise Manager is the reporting and configuration interface and Foundstone Security Factors™ aids in evaluating risk levels. Foundstone's products are built around their lifecycle approach as depicted below.

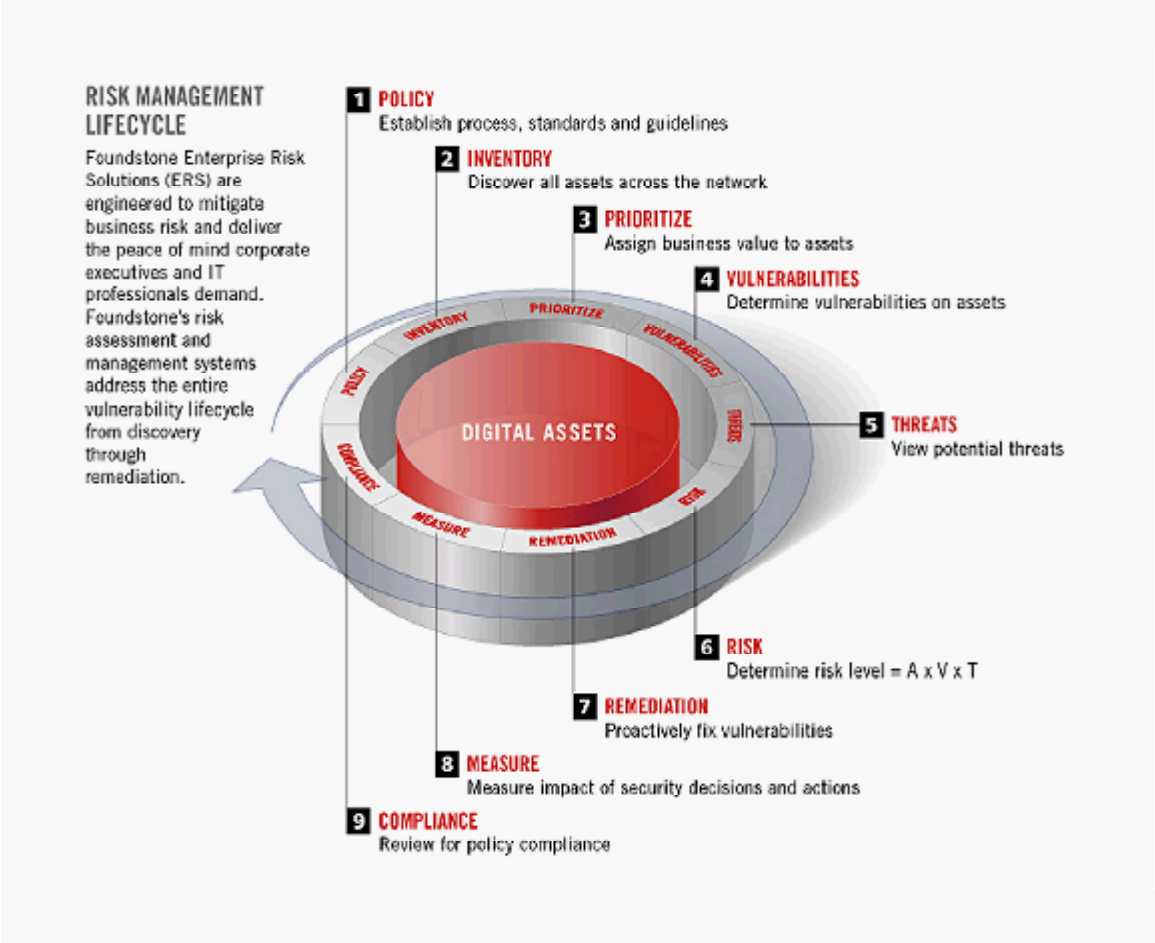


Figure 2 Foundstone Risk Management Lifecycle
http://www.foundstone.com/index.htm?subnav=products/navigation.htm&subcontent=/products/overview.htm

Strengths

Like Latis VAM, Foundstone is deployed in a distributed fashion for the same reasons. As well, the scan engine will also tailor the scanning policy to the device being assessed. Foundstone also has the ability to scan in defined windows, pausing or stopping the assessment once the window has expired. For the remediation component, Foundstone utilizes the Foundstone Security Factors™, which includes the ability to assign a risk score to devices based on their level of importance. This aids in presenting the highest risk issues first for mitigation. Once vulnerabilities are identified, they are reported in the Enterprise Manager, assigned to owners and tracked to remediation. An example of a closed ticket is shown below. Note the status and verified fields which show that the issue did indeed pass verification. Foundstone also allows users to verify fixes based on their roles, which can be done either automatically or scheduled. Notifications can be sent to the responsible users whenever new vulnerabilities are found, or when vulnerabilities are removed. In addition, reports can be created based on any logical grouping.

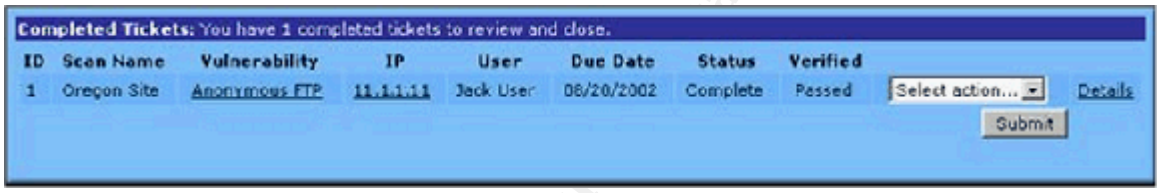


Figure 3 Foundstone Completed Ticket

Areas for Improvement

While reporting in the web interface is excellent, the ability to export reports to other formats is not supported at this time.

Tenable Network Security Lightning

Tenable's Lightning solution is comprised of 3 components: the Lightning console, the Lightning Proxy, and Nessus network scanners. The Lightning console is used for reporting and configuration while the Lightning Proxy is used to consolidate your Nessus scanners into logical groupings.

Strengths

Just as the aforementioned products, Tenable is deployed in a distributed fashion; however, unlike the others, the Nessus scanners can be arranged in groups to report to a Lightning Proxy. Each proxy server learns which network it has the capability to assess. This allows the proxy to engage the appropriate scanners to perform the assessment. As well, this allows multiple scanners to perform the scan if they have coverage of the same network address space thereby increasing the speed of the scan. Tenable also allows vulnerabilities to be tracked to remediation, not only tracking the end user's comments, as shown below, but also the security administrator's recommendations. Lightning also allows users to scan for verification of issues based on role assignments. Lightning supports the ability to define scan windows. If the scan exceeds the

defined window, it will be halted. In addition, Lightning allows you to configure emails to be sent at the start and stop of scans. This can aid in notifying IT personnel of your activity, such as a network operations center. Although Lightning is a web interface, reports can be exported as PDF. As a bonus, Lightning offers the ability to correlate data from several intrusion detection systems against your vulnerability data generating email alerts as they occur.

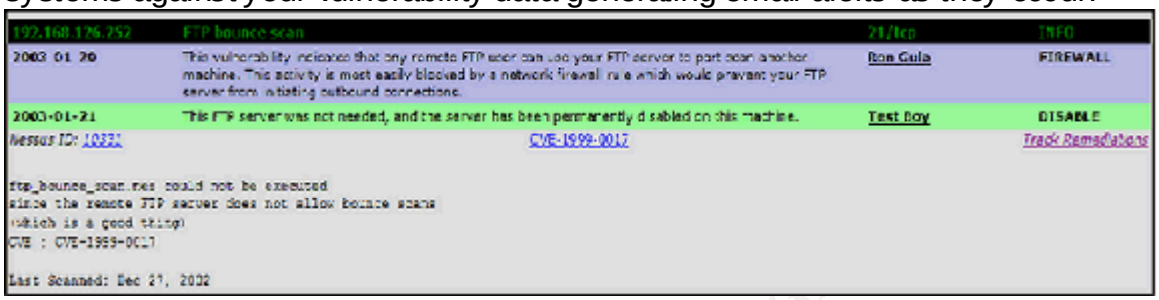


Figure 4 Tenable Network Security Lightning Console Recommendation/Remediation View

Areas for Improvement

Tenable's solution does not offer the ability to risk weight your assets; therefore, prioritization of issues will be a problem.

Decision Points

All three of the products reviewed above are excellent contenders into the newly created vulnerability management space. In order to provide the most value to the organization, you must consider your existing infrastructure. This may include any vulnerability assessment tools you have in place, and, or the hardware they reside on. For both Latis and Tenable, if you have an existing Nessus infrastructure, the ability to implement their products will be minimal as you can utilize your existing hardware and policies. If you are deploying a new infrastructure, all three vendors either currently have, or will offer a scanning appliance by mid year. In addition, the reporting engine and configuration interface for all three products is web based. This will require the ability to setup and maintain a web server of some type. As well, two of the three products, Latis and Foundstone, require an SQL database, which will add additional overhead for maintenance.; however, that also adds the ability to create your own SQL based reports.

Conclusion

Vulnerability assessment is a necessary activity within many organizations. To help improve the effectiveness of your program, there are two areas that can be targeted: the impact to your environment and the ability to manage the flow of your assessment data. To help reduce the impact to your environment you need to keep the following items in mind:

- ✓ Communication of the program
- ✓ Use of appropriate change and enterprise management
- ✓ Placement of your assessments tools where they provide the most value

- ✓ Tuning of your assessment policy
- ✓ Automation of the assessments

All three of the products reviewed are excellent contenders into the newly created vulnerability management space. Combine any of these tools with the elements of reducing impact and you are sure to increase your return on investment, in time, capital and human resources. In addition, these tools allow you to show a full lifecycle of risk management which provides the relevant metrics to senior management that the risk is actually being reduced.

References

Armstrong, Illena. "Hackers: Are you inviting them in?" SC Magazine. January, 2003. <http://www.scmagazine.com/scmagazine/2003_01/feature_1/>

Armstrong, Illena. "Vulnerability Testing: Keeping a tight ship" SC Magazine. February, 2003. <http://www.scmagazine.com/scmagazine/2003_02/feature_2/>

Berg, Al. "Vulnerability Management: Feeling Vulnerable" Information Security Magazine. February, 2002. <http://www.infosecuritymag.com/2002/feb/features_vulnerable.shtml>

Gula, Ron. "Dedicated and Distributed Vulnerability Management". March 2003. <http://www.tenablesecurity.com/distributed.pdf>. 8-9.

Krutz, Ronald L. and Vines, Russell Dean. The CISSP Prep Guide. Indianapolis: Wiley Publishing Inc., 2003. 11-12, 16-19.

Snyder, Joel. "How Vulnerable?" Information Security Magazine. March, 2003. <http://www.infosecuritymag.com/2003/mar/cover.shtml>

Latis Networks Inc. <http://www.latis.com/products/svam/vam1.html> Superior, Colorado: Latis Networks Inc., 2003.

Foundstone Inc. <http://www.foundstone.com/index.htm?subnav=products/navigation.htm&subcontent=/products/overview.htm> Mission Viejo, California: Foundstone Inc., 2003.

Tenable Network Security Inc. < http://www.tenablesecurity.com/> Columbia, Maryland: Tenable Network Security Inc., 2002-2003.

Last Updated: May 28th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Madrid 2017	Madrid, ES	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GAUS	May 30, 2017 - Jun 04, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CAUS	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DCUS	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TXUS	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Milan 2017	Milan, IT	Jun 12, 2017 - Jun 17, 2017	Live Event
SEC555: SIEM-Tactical Analytics	San Diego, CAUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NCUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, NL	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, COUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MNUS	Jun 19, 2017 - Jun 24, 2017	Live Event
DFIR Summit & Training 2017	Austin, TXUS	Jun 22, 2017 - Jun 29, 2017	Live Event
SANS Paris 2017	Paris, FR	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, AU	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MDUS	Jun 26, 2017 - Jul 01, 2017	Live Event
SEC564:Red Team Ops	San Diego, CAUS	Jun 29, 2017 - Jun 30, 2017	Live Event
SANS London July 2017	London, GB	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, JP	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, SG	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CAUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS ICS & Energy-Houston 2017	Houston, TXUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, DE	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DCUS	Jul 22, 2017 - Jul 29, 2017	Live Event
Security Awareness Summit & Training 2017	Nashville, TNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, ILUS	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, AU	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Stockholm 2017	OnlineSE	May 29, 2017 - Jun 03, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced