Global Information Assurance Certification Paper

Implementing a vulnerability management process

GIAC (GSEC) Gold Certification

Author: Tom Palmaers, tom@palmaers.be
Advisor: Dennis Distler

Accepted: 03/23/2013

Abstract

This paper looks at how a vulnerability management (VM) process could be designed & implemented within an organization. Articles and studies about VM usually focus mainly on the technology aspects of vulnerability scanning. The goal of this study is to call attention to something that is often overlooked: a basic VM process which could be easily adapted and implemented in any part of the organization.

1. Introduction

A vulnerability is defined in the ISO 27002 standard as "A weakness of an asset or group of assets that can be exploited by one or more threats" (International Organization for Standardization, 2005)

Vulnerability management is the process in which vulnerabilities in IT are identified and the risks of these vulnerabilities are evaluated. This evaluation leads to correcting the vulnerabilities and removing the risk or a formal risk acceptance by the management of an organization (e.g. in case the impact of an attack would be low or the cost of correction does not outweigh possible damages to the organization).

The term vulnerability management is often confused with vulnerability scanning. Despite the fact both are related, there is an important difference between the two. Vulnerability scanning consists of using a computer program to identify vulnerabilities in networks, computer infrastructure or applications. Vulnerability management is the process surrounding vulnerability scanning, also taking into account other aspects such as risk acceptance, remediation etc.

1.1. Why Vulnerability Management is required?

The increasing growth of cyber-crime and the associated risks are forcing most organizations to focus more attention on information security. A vulnerability management process should be part of an organization's effort to control information security risks. This process will allow an organization to obtain a continuous overview of vulnerabilities in their IT environment and the risks associated with them. Only by identifying and mitigating vulnerabilities in the IT environment can an organization prevent attackers from penetrating their networks and stealing information (Williams and Nicollet, 2005).

1.2. Vulnerability Scanners

As vulnerability management is the process surrounding vulnerability scanning, it is important to understand how vulnerability scans are performed and what tools that are available. Today, the level of technical expertise required to operate a vulnerability

scanning tool is low. The majority of vulnerability scanners can be controlled using a GUI allowing a user to launch vulnerability scans against an entire network with a few mouse clicks.

Several vendors provide a variety of technical solutions, with different deployment options. These deployment options include standalone, managed services or even software as a service (SaaS). Some of the vendors offering vulnerability scanning technology include: McAfee, Qualys, Rapid 7, Tenable Network Security as well as a few open source projects.

It's recommended an organization thoroughly tests vulnerability scanning products before deciding which solution best meets the requirements of the organization. Attention should be paid to the fact that scanning a single box with multiple products using their default settings could produce very different results. No matter which vulnerability scanning solution is selected, it's important to properly configure and tune scans to limit the amount of false positives in the scan results.

1.3. Associated risks

There is some risk involved with vulnerability management or more specifically, vulnerability scanning. Since vulnerability scanning typically involves sending a large number of packets to systems, they might sometimes trigger unusual effects such as – for example - disrupting network equipment. However, since vulnerability scanning is mainly limited to scanning and not exploiting, risks are minimal.

In order to cover these risks, it's always important to inform various stakeholders within your organization when vulnerability scanning is taking place.

2. A Vulnerability Management Process

2.1. Objective

The main objective of a vulnerability management process is to detect and remediate vulnerabilities in a timely fashion (Qualys, 2008). Many organizations do not frequently perform vulnerability scans in their environment. They perform scans on a quarterly or annual basis which only provides a snapshot at that point in time. The figure below shows a possible vulnerability lifecycle with annual scanning in place:

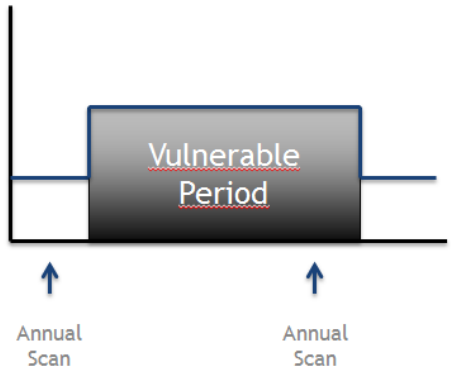

Figure 1: Vulnerability scanning

Any vulnerability not detected after a schedule scan takes place, will only be detected at the next scheduled scan. This could leave systems vulnerable for a long period of time. When implementing a vulnerability management process, regular scans should be scheduled to reduce the exposure time. The above situation will then look like this:

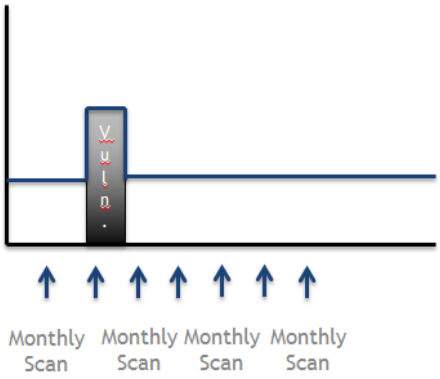

Figure 2: Continuous vulnerability management

Regular scanning ensures new vulnerabilities are detected in a timely manner, allow them to be remediated faster. Having this process in place greatly reduces the risks an organization is facing.

2.2. Roles and responsibilities

When building a vulnerability management process, the following roles should be identified within the organization:

a) Security Officer: The security officer is the owner of the vulnerability management process. This person designs the process and ensures it is implemented as designed.

b) Vulnerability Engineer: The vulnerability engineer role is responsible for configuring the vulnerability scanner and scheduling the various vulnerability scans.
c) Asset Owner: The asset owner is responsible for the IT asset that is scanned by the vulnerability management process. This role should decide whether identified vulnerabilities are mitigated or their associated risks are accepted.
d) IT System Engineer: The IT system engineer role is typically responsible for implementing remediating actions defined as a result of detected vulnerabilities.

2.3. Vulnerability Management Process: Step-by-Step

A vulnerability management process consists of five phases:

- Preparation
- Vulnerability scan
- Define remediating actions
- Implement remediating actions
- Rescan

2.3.1. Preparation

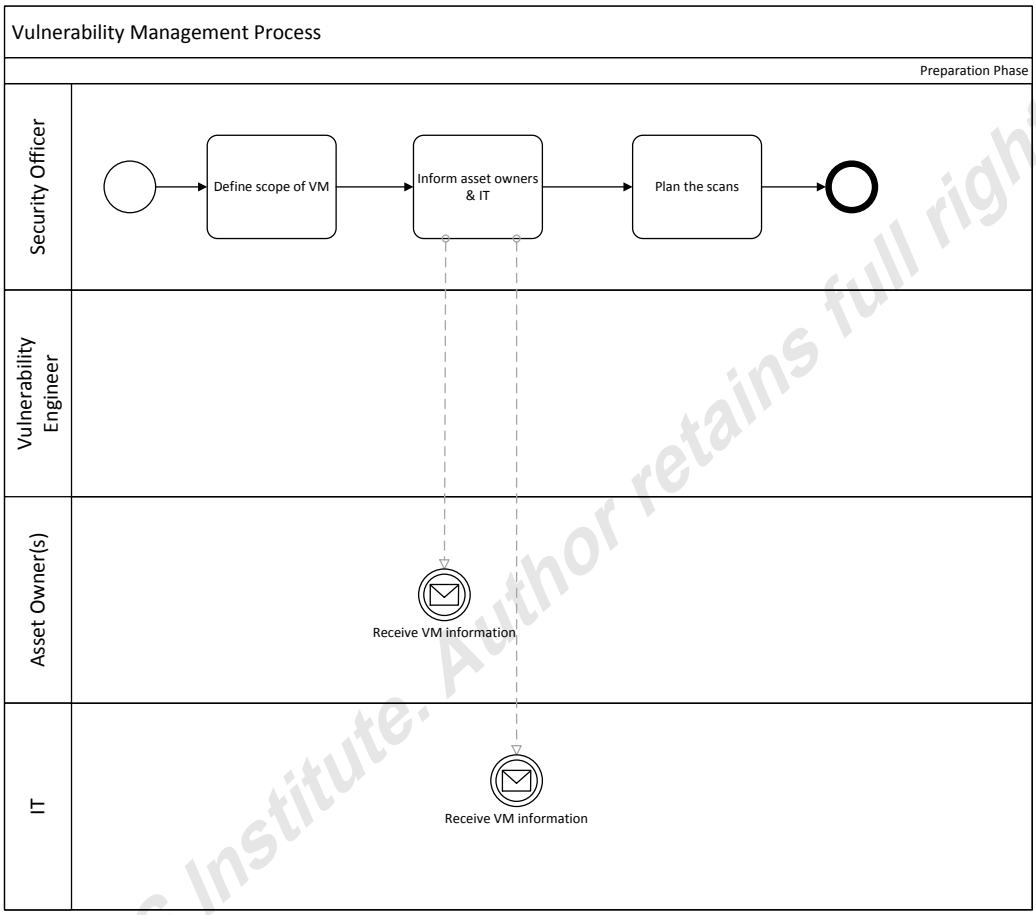

Figure 3: Vulnerability Management - Preparation phase

The preparation phase is the first phase in a vulnerability management process. To prevent being overwhelmed by thousands of vulnerabilities identified in the first scans, it is recommended to start with a small scope. This can be achieved by starting out with a small number of systems or by limiting the number of vulnerabilities identified by the vulnerability scanner (e.g. only scan for vulnerabilities for which a known exploit granting remote access exists).

The preparation phase is mainly the responsibility of the Security Office in an organization. The first step is to define the scope of the vulnerability management process. It is important to obtain an agreement which systems will be included or excluded from the vulnerability management process. Besides the in scope systems, an organization should also determine the type of scans. Possibilities can include either an external scan performed from the perspective of an external attacker on the internet or an

internal scan from the perspective of an attacker on the internal network. Both types of scans can be either unauthenticated or authenticated scanning.

An external scan provides an overview of security vulnerabilities which are visible from outside a network, taking into account all security layers on the network between the scanner machine and the target system. This controls can include includes network firewalls, intrusion detection systems, (web) application firewalls as well as any host based security controls which are present on the target system. The results of an external scan give an indication on the correct configuration of the network security controls between the scanner and the target system.

A scan performed from the internal network, provides an overview of vulnerabilities which are visible from the local network, taking into account host based security controls that are present on the target system. By performing an internal scan of each component in an architecture, the results can provide information on how well each layer is secured. ("defense in-depth")

Both external and internal scans can be executed using authentication. In those cases, the scanning technology will authenticate itself to the target system using valid credentials in order to extract additional information from the system that would otherwise not be accessible. This information includes specific security configurations and software patch levels. Using authenticated scanning will result in more accurate and complete vulnerability scanning reports.

While each scan type has their own advantages, vulnerability management processes usually use a combination of both. Security officers should in the long term work towards performing internal scans on every component of the infrastructure.

When determining the scope of systems to include in the vulnerability management process, it is usually not feasible to include everything in the first iteration of vulnerability scanning. The rule of thumb should be to start small. This will ensure the number of vulnerabilities discovered will be manageable. A risk based approach should be used to determine the scope for an initial vulnerability scan. There are several ways to approach this. Some organizations see external threats as the biggest risk and would start with a scope consisting of internet facing systems. Other organizations think their

company information is at risk and will start with a limited scope of systems containing such information.

When implementing a vulnerability management process, it is recommended to start out with a small scope. The small scope will allow the stakeholders involved to focus on implementing the process and prevent them from being overwhelmed with vulnerability information from hundreds or thousands of systems.

Once the scope has been determined, the security officer should inform relevant asset owners in the organization. These people are accountable or responsible for the systems. The asset owner is responsible for identifying remediating actions to mitigate the identified vulnerabilities. In most situations, asset owners should make these decisions after examining the recommendations and risk assessment prepared by the security officer. It is important to obtain buy-in from asset owners within an organization. It is recommended to inform them about upcoming vulnerability scans. The objectives of the vulnerability management process should be explained to them in detail, including how this process affects the systems they are responsible for. Additionally what their responsibilities are in the whole process should be explained. Depending on system criticality, asset owners may have specific requirements such as not scanning production systems outside of maintenance windows or only performing scans during business hours. Depending on the organization and the mandate of the security officer, it may be necessary to obtain formal approval from each asset owners before performing vulnerability scans.

Informing IT, specifically teams managing firewalls, IDS or other security monitoring systems, should be part of any vulnerability management process. The alerting on such systems is often triggered by vulnerability scanning tools, so it's important to ensure these teams are aware of the vulnerability scans.

The last step of the preparation phase consists of planning the vulnerability scans. Depending on the scan configuration which includes the number of vulnerability checks, authentication scan type, and applications installed on the target, a vulnerability scan against a single IP address can take between a few minutes to a few hours. In case it is unclear how long a certain scan could last, it is recommended to perform a test scan on a

similar test environment. This will provide an estimate on long these scans will take and their impact on the network.

The following table shows an example of how all information needed to perform the scans can be gathered in a planning spreadsheet. A planning spreadsheet could look like this:

IP Range	Business Owner	Department	Planned Date	Contacts
192.168.1.0/24	Robot Control Systems	Manufacturing	16/jan/13	manuf@company.com
192.168.2.0/24	Company Web Servers	Marketing	17/jan/13	marketing@company.com
192.168.3.0/24	Email Servers	Internal IT	18/jan/13	it@company.com

Figure 4: Planning spreadsheet

The risk appetite of the organization plays an important role in the vulnerability management process. If an organization is willing to ignore some risks (e.g. due to limited resources being available), the scope of the vulnerability management process can stay limited, e.g. only high risks for which known exploits exist. Organizations that want to obtain a clear understanding of each vulnerability in their environment and their associated risks should, with each iteration of the process, increase the scope and grow towards their desired scope.

2.3.2. Initial vulnerability scan

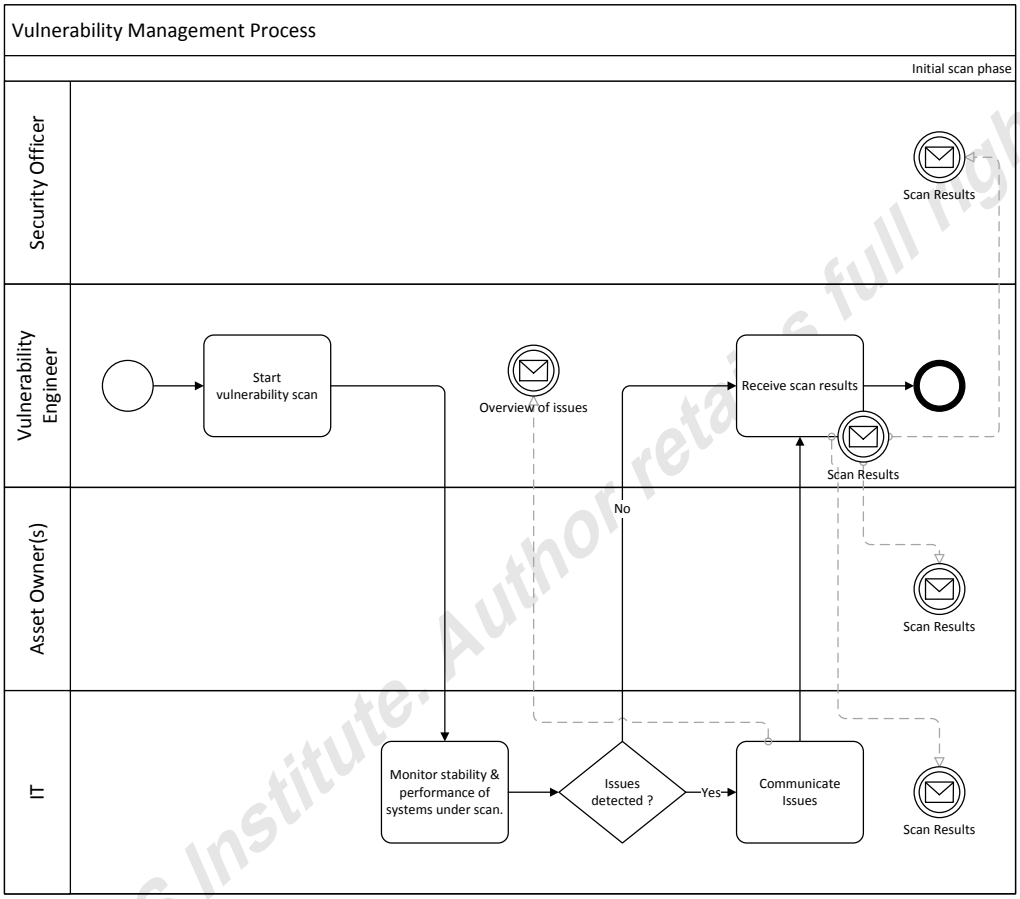

Figure 5: Vulnerability Management Process - Initial scan phase

Once the preparation phase is complete, the next phase of the process begins and the initial vulnerability scans are performed. Any issues which occurs during the scans, for example systems becoming unavailable or poor application response, should be recorded since this may happen again in the future. In this case, actions may be defined to reduce the impact of future scans on the stability or performance of the target systems.

Most vulnerability scanning tools offer a wide range of reporting options to visualize scan results. It is necessary to use them to create a various number of reports. Management and the security officer will be interested in the risk the organization is currently facing, this risk includes number of vulnerabilities detected and the severity/risk rating of the identified vulnerabilities. Asset owners will want to obtain an overview of vulnerabilities in the systems they are responsible for. The IT department will want an

overview (per technology) of technical information about detected vulnerabilities as well as recommendations for mitigation and improvement.

2.3.3. Remediation phase

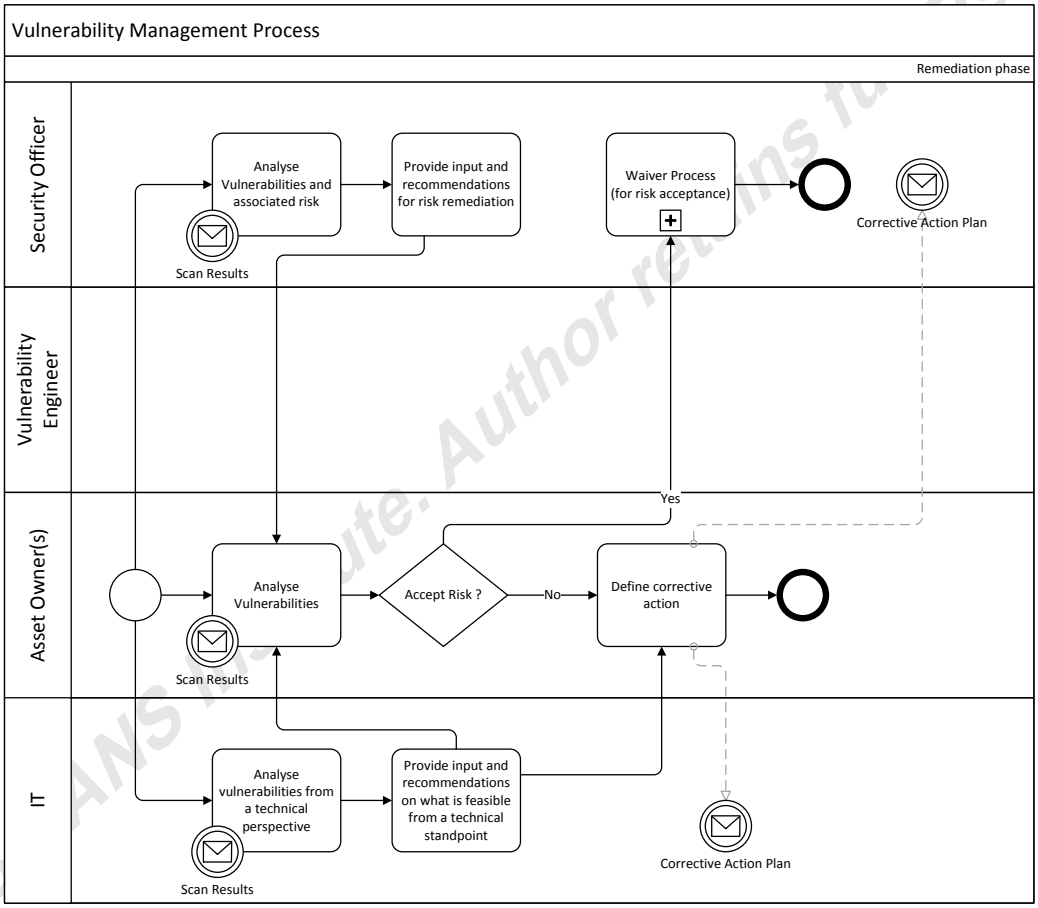

Figure 6: Vulnerability Management Process - Remediation phase

In the next phase, the asset owners, with the cooperation of the security officer and the IT department, will define remediating actions. The security officer will analyze the vulnerabilities, determine the associated risks and will provide input on risk remediation. The IT department will analyze the vulnerabilities from a technical perspective and answer questions such as if patches are available or whether the configuration can be hardened ? The IT department recommendation also includes the feasibility of the possible remediating action such as whether installing a certain patch will result in the application no longer be supported by the vendor. In order to ensure

remediation is given sufficient priority the security officer should set clear deadlines when the remediating actions will be implemented. Asset owners should include a timeline in their action plan indicating when these remediating actions will be implemented. The remediation timeframe should be in line with the level of risk detected. This timeframe will be different for each organization since the reaction speed will depend greatly on the risk appetite of the organization. The below table contains an example overview of possible mitigation timeframes depending on the type of risk:

L	Scan Date	Vulnerability Detected	Risk Rating	Corrective Action	Implementation Date
192.168.4.56	1/02/2013	PHP "safe mode" - Restriction Bypass Vulnerability	4	PHP upgrade. This can only be deployed after code migration is complete.	15/12/2013
192.168.4.56	1/02/2013	Apache prior to 2.2.15 - Multiple vulnerabilities	4	Upgrade apache to newer version	15/02/2013

Figure 7: Overview of possible mitigation timeframe

The security officer keeps track of planned remediating actions in order to follow up on their implementation. This can be done by using a simple spreadsheet. Another way of tracking remediation is the implementation of relevant registered changes in the service desk system. Finally, some vulnerability scanners contain specific modules that also allow tracking the status of remediating actions.

If short term remediation is not possible, compensating controls should be identified in order to mitigate/remove the risk without correcting the vulnerability. Such compensating controls could include restricting network access to the vulnerable service, virtual patching, etc.

In case asset owners decide to accept the risk, it should be documented through a risk acceptance process. A risk acceptance or waiver process is a formal process in which an exception to the security policies can be requested. This request is analyzed with regards to risks the organization would be exposed to if the exception is granted. If possible, compensating controls to remediate these risks are proposed. In the final step of a risk waiver process, the asset owner analyses the risks, whether or not compensating controls can be foreseen (Wheeler E, 2011). This allows the asset owner to make thoughtful decisions with regards to accepting the risk. The ability to signoff is determined based on the level of risk. Usually high risks can only be accepted by management of an organization, whereas small risks can be accepted by asset owners.

Risk waivers should always be limited in time to ensure these risks are revaluated on a regular basis (e.g. annually).

2.3.4. Implement remediating actions

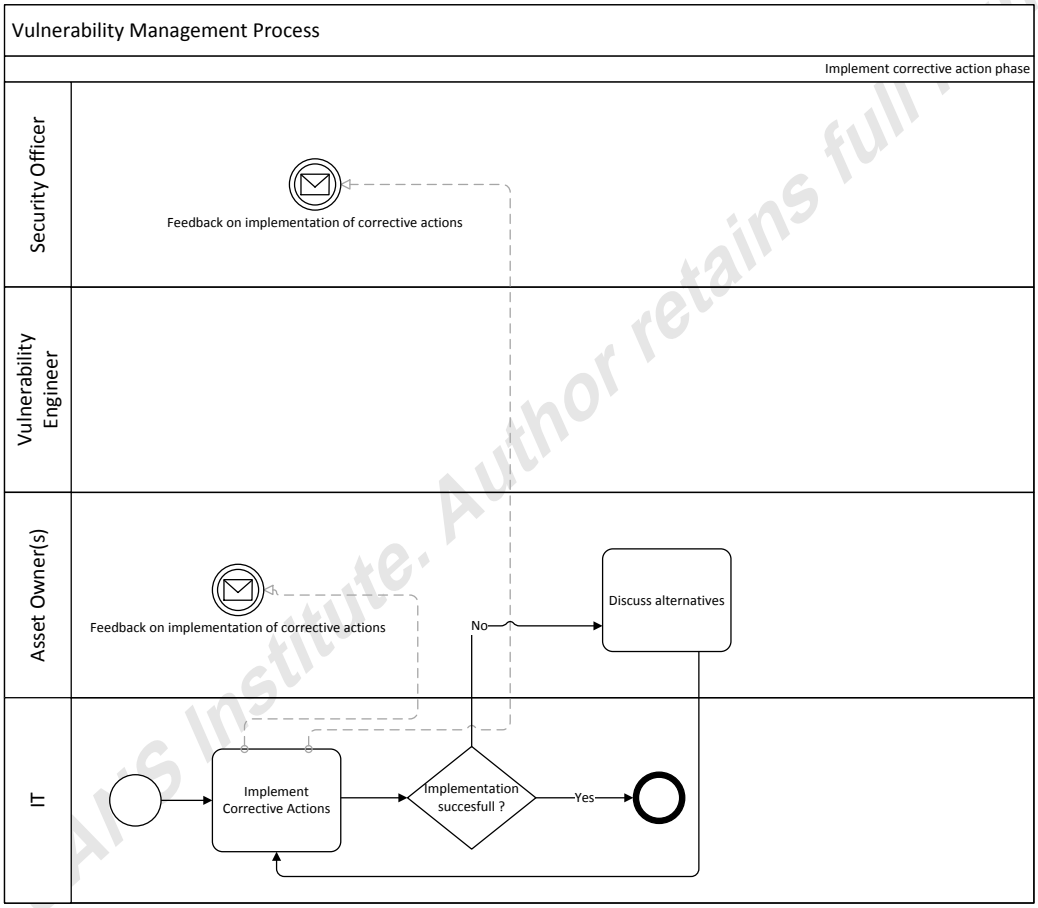

Figure 8: Vulnerability Management Process – Implement remediating actions

The planned remediating actions should be executed in line with the agreed timeframes. If a problem occurs with implemented remediation, it should be recorded. Alternative actions should be defined by the asset owner based on recommendations by the security officer and the IT department. These new or other remediating actions should then be implemented. The security officer should track the status of the remediating actions.

2.3.5. Rescan

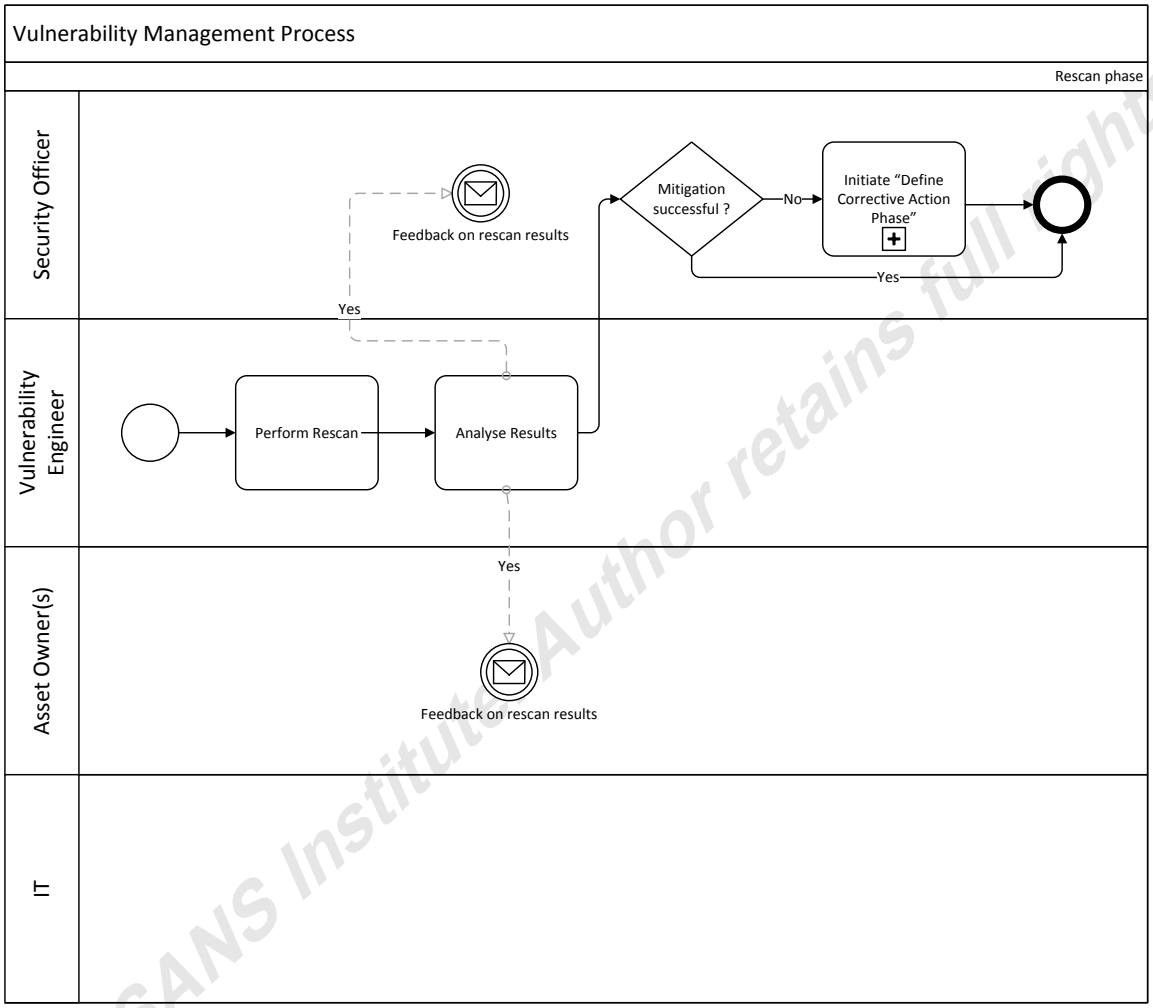

Figure 9: Vulnerability Management Process - Rescan phase

Once a vulnerability is remediated, a rescan has to be scheduled to verify the remediating actions have been implemented. This scan will be performed using the same vulnerability scanning tools and identical configuration settings as the initial scan. This step is very important to prevent inaccurate results due to configuration errors. Typically a rescan is scheduled after the deadline for implementing remediating actions.

For these scans, the same types of reports generated during the initial scan are created. For follow-up, management and asset owners will be interested to know whether the remediating actions have been effectively implemented and whether any residual risk remains. The IT department will be interested in how effective the remediating actions have been implemented.

The next step is an agreement between asset owners and the security officer on how often such scans will be scheduled. This timeframe should take into account the risk appetite of the organization, as well as the capability of the organization to remediate identified vulnerabilities. In order to establish a mature vulnerability management process, it is recommended to schedule scans frequently, typically on a weekly or monthly basis. This will ensure rapid detection of vulnerabilities, allowing the organization to determine and deploy mitigating controls in a timely fashion.

Correcting vulnerabilities from the initial scan provide good insight into the ability of the (IT) organization to handle requests. Furthermore, lessons learned during the execution of the process should be used to reevaluate and improve the vulnerability management process.

3. Real world applications: an example

To demonstrate the implementation of a vulnerability management process, a lab environment with two machines will be used. The first machine is running Metasploitable, a Linux system intentionally containing numerous vulnerabilities. The other machine is a scanning machine running the latest version of Nessus. Vulnerability updates for Nessus are acquired using the free (for home use) Home Feed.

Since in this paper the focus is on a vulnerability management process should be implemented, not every technical command is included in this simulation.

3.1.1. Preparation phase

The first step in applying the vulnerability management process is the preparation phase. The scope of the exercise consists out of a single server machine with the IP 192.168.2.191. Since it is the first time such an exercise is being performed, it is agreed to only focus on vulnerabilities rated as "Critical" by the vulnerability scanner. The planning spreadsheet would looks like this:

IP Range	Business Owner	Department	Planned Date	Contacts
192.168.2.191/32	John Doe	IT	14/feb/13	john.doe@company.com

Figure 10: Planning spreadsheet used in Lab exercise

The asset owner and IT are notified of the planned scanning date and timeframe. It should be noted in this example the asset owner and IT is the same department.

In the preparation phase the vulnerability scanner is configured. In this example, one of the Nessus preconfigured scanning policies named "Internal Network Scan" will be used. This policy is tuned for scanning large internal networks and specifically looks for exposed services that are typically found on an internal network. (Tenable Network Security, 2013 & Carey, Rogers, Cricuolo and Petruzzi, 2009)

3.1.2. Initial Vulnerability Scan

As scheduled the initial vulnerability scan is launched. Launching a scan in Nessus can be performed by logging in in the Nessus web interface, selecting "Add

Scan" and then enter the target IP addresses (in this example 192.168.2.191) in the scan targets box, as shown in the figure below.

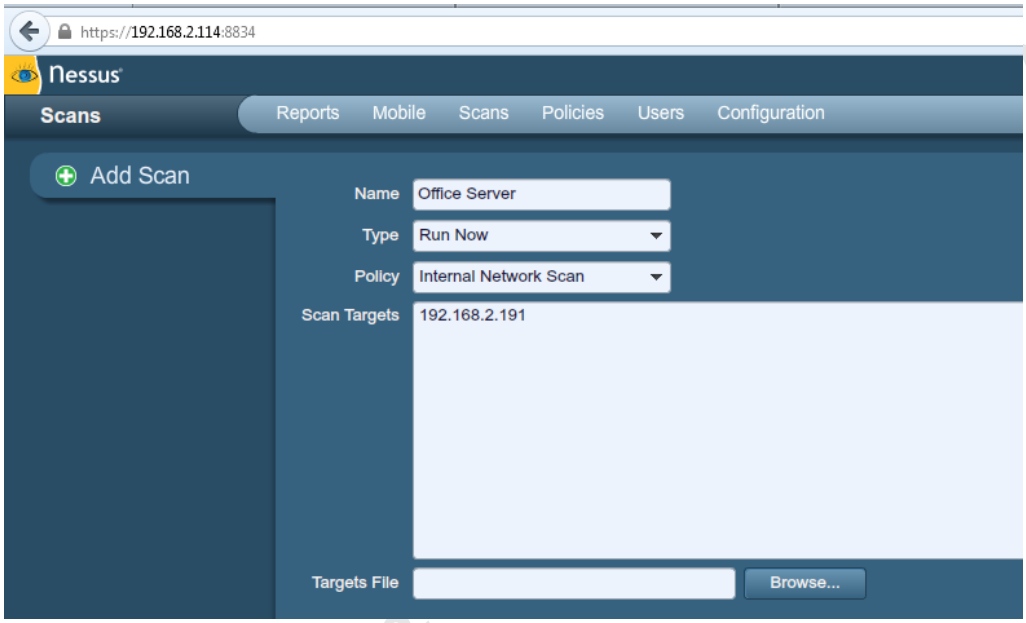

Figure 11: Nessus - Add Scan configuration used in Lab exercise

The scanning policy to be used is the "Internal Network Scan" policy. After all relevant scan information is entered, clicking the "Submit" button will immediately launch the vulnerability scan.

Once the scan is complete, scan results are available through the "Reports" menu of Nessus. In the screenshots below a number of vulnerabilities have been detected in our target system are shown. Six detected vulnerabilities have been rated as critical by the Nessus vulnerability scanner.

Office Server Vulnerability Summary | Host Summary
Completed: Jan 31, 2013 14:30
Download Report
Remove Vulnerability | Audit Trail
Filters No Filters Add Filter Clear Filters

Plugin ID	Count	Severity	Name	Family
10380	1	Critical	rsh Unauthenticated Access (via finger Information)	Gain a shell remotely
25216	1	Critical	Samba NDR MS-RPC Request Heap-Based Remote Buffer Overflow	Misc.
32314	1	Critical	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	Gain a shell remotely
51988	1	Critical	Rogue Shell Backdoor Detection	Backdoors
55523	1	Critical	vsftpd Smiley Face Backdoor	FTP
61708	1	Critical	VNC Server 'password' Password	Gain a shell remotely
10205	1	High	rlogin Service Detection	Service detection
10245	1	High	rsh Service Detection	Service detection
10481	1	High	MySQL Unpassworded Account Check	Databases
33447	1	High	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning	DNS
42411	1	High	Microsoft Windows SMB Shares Unprivileged Access	Windows
10056	1	Medium	/doc Directory Browsable	CGI abuses
10079	1	Medium	Anonymous FTP Enabled	FTP
10203	1	Medium	rexecd Service Detection	Service detection
11213	1	Medium	HTTP TRACE / TRACK Methods Allowed	Web Servers
12217	1	Medium	DNS Server Cache Snooping Remote Information Disclosure	DNS
15901	1	Medium	SSL Certificate Expiry	General
20007	1	Medium	SSL Version 2 (v2) Protocol Detection	Service detection
26928	1	Medium	SSL Weak Cipher Suites Supported	General
31705	1	Medium	SSL Anonymous Cipher Suites Supported	Service detection
42256	1	Medium	NFS Shares World Readable	RPC

Figure 12: Nessus - Results of "Office Server" scan in Lab exercise

3.1.3. Define Corrective Actions or Accept Risk

In the next phase, the vulnerabilities and their possible impact are analyzed. After analyzing the six critical vulnerabilities, management of the organization decided to remediate two vulnerabilities, the detected Rogue Shell backdoor, and changing the default VNC server password.

Remediation of the Rogue Shell backdoor vulnerability includes identifying the process containing the backdoor, deactivating it and removing it from the system. For the remediation of the VNC password, IT informs the security officer the VNC password cannot be changed at the moment since because it is used by a service desk automated processes. IT state's the password can be changed as of June, 1st 2013. Based on the feedback received from the asset owner and IT, the Security Officer documents the decisions. Hereby an example of a spreadsheet to track these decisions:

L	Scan Date	Vulnerability Detected	Risk Rating	Corrective Action	Implementation Date
192.168.2.191	14/02/2013	Rsh unauthenticated access	Critical	None, risk waiver approved by management	N/A
192.168.2.191	14/02/2013	Samba NDR MS-RPC Request Heap-Based Remote Buffer Overflow	Critical	None, risk waiver approved by management	N/A
192.168.2.191	14/02/2013	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	Critical	None, risk waiver approved by management	N/A
192.168.2.191	14/02/2013	Rogue Shell Backdoor detection	Critical	Disable & remove backdoor from system	21/02/2013
192.168.2.191	14/02/2013	Vsftpd Smiley Face backdoor	Critical	None, risk waiver approved by management	N/A

192.168.2.191	14/02/2013	VNC Server 'password' Password	Critical	Password will be changed to a secure password	18/06/2013

Figure 13: Tracking spreadsheet used in Lab exercise

All risk waivers are formally documented and signed off by the management of the organization.

3.1.4. Implement Corrective Actions

In this phase, the remediating actions which have been defined are implemented. The backdoor on the system is deactivated and remediating actions are executed. In our example the xinetd configuration is cleaned up to prevent the backdoor from starting again. Since it was decided not to change the VNC server password at this time, all planned remediating actions have been performed.

3.1.5. Rescan

The last phase consists of rescanning the machines in the original scope using the same scanning configuration. As seen from the rescanning results in the screenshot below, the Rogue shell backdoor vulnerability is no longer present.

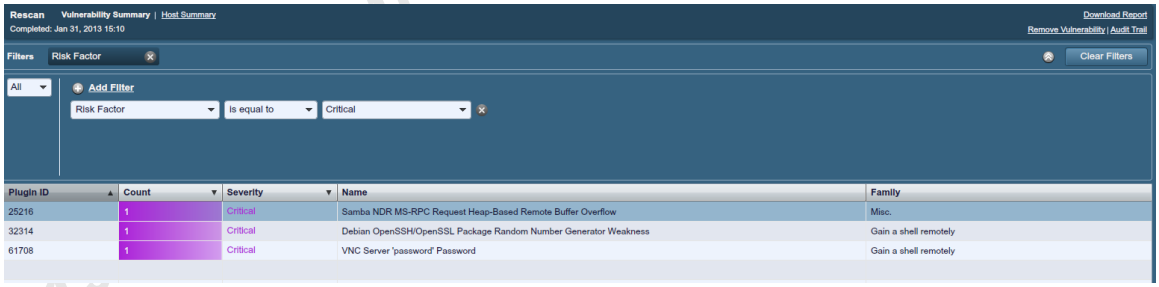

Figure 14: Lab exercise - Rescan results

4. Conclusions

Without a vulnerability management process in place, the management of an organization is blind to risks related to the security of the IT infrastructure. Implementing a vulnerability management process is all about managing risk. By having a well-defined process in place, an organization can obtain a continuous view of the risk associated with the presence of security vulnerabilities in its IT systems. This allows management to take well-advised decisions with regards to remediating actions that could be implemented to reduce the risks. In short, any organization that wants to obtain an understanding of the

security risks they are facing due to the technology they are using should implement a vulnerability management process.

However, introducing a new vulnerability management process within an organization can also be challenging. In order to ensure a successful vulnerability management program, attention should be paid to a number of aspects. First of all roles and responsibilities should be clearly assigned. Ensure all stakeholders within the organization know what to expect. Then select a vulnerability scanning technology that suits the needs of your organization. Sufficient attention should be paid to the configuration and fine tuning of the vulnerability scanner technology. Finally, when starting out with vulnerability management, it is recommended to limit the scope of the initial vulnerability scans. This prevents initial scans that result in tens of thousands of vulnerabilities. A better approach would be to only select a limited set of vulnerabilities (such as the SANS TOP 10) or only those that are marked as “high risk” by the vulnerability scanner tool.

5. References

ISO/IEC, "Information technology -- Security techniques – Code of practice for information security management " ISO/IEC 27002

Qualys, . *Vulnerability management for dummies*. Chichester: John Wiley & Sons, 2008. eBook.

Williams, A and Nicollet, M: *Improve IT Security With Vulnerability Management*, Gartner ID Number: G00127481, May 2005

Carey, M., R. Rogers, P. Criscuolo, and M. Petruzzi. *Nessus network auditing*. 2. Burlington, MA: Syngress Media Inc, 2009. Print.

Wheeler, E. *Security risk management, building an information security risk management program from the ground up*. Syngress, 2011. Print.

Mell P, Bergeron T, Henning D. *NIST Special Publication 800-40: Creating a patch and vulnerability management program.* Retrieved from http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf

Tenable Network Security. (2013) *Nessus 5.0 User Guide.* Retrieved from http://static.tenable.com/documentation/nessus_5.0_user_guide.pdf

Wikipedia. *Vulnerability Management*. Retrieved from http://en.wikipedia.org/wiki/Vulnerability_management

Brenner, B. *Vulnerability management: The basics.* Retrieved from http://www.csoonline.com/article/611067/vulnerability-management-the-basics

Stiennon, R. *Vulnerability Intelligence vs. Vulnerability Management*. Retrieved from http://www.forbes.com/sites/richardstiennon/2012/07/26/vulnerability-intelligence-versus-vulnerability-management/