Interested in learning more about security?

SANS Institute InfoSec Reading Room

Applying Lessons Learned for the Next Generation Vulnerability Management System

Vulnerability management has been defined as the "cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities," (Cornell, 2009) especially in software and firmware. As such, it is integral to "Information Assurance" for most organizations with networks. In order to conduct vulnerability management, many organizations, such as the United States Department of Defense (DoD), have created systems such as the Vulnerability Management System (VMS). However, the current v...

Applying Lessons Learned for the Next Generation Vulnerability Management System

GIAC Gold Paper

Author: John Dittmer, jdittmer@suprtek.com

Advisor: Chris Walker

Accepted: June 3, 2015

Abstract

Vulnerability management has been defined as the "cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities," (Cornell, 2009) especially in software and firmware. As such, it is integral to “Information Assurance” for most organizations with networks. In order to conduct vulnerability management, many organizations, such as the United States Department of Defense (DoD), have created systems such as the Vulnerability Management System (VMS). However, the current version of VMS is very cumbersome and it is about to be replaced by the Continuous Monitoring and Risk Scoring (CMRS) system. CMRS will integrate several Information Assurance activities with vulnerability management. However, there is room for improvement, even with the implementation of the new system. This paper will offer solutions for improving the vulnerability management process with either improvement to future versions of CMRS or other future systems.

John Dittmer, jdittmer@suprtek.com

1. Introduction

The objective of this paper is to recommendations for improving a vulnerability management system in development.[1] On a daily basis, information security personnel have to remediate or mitigate security vulnerabilities. Formally defined, vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source (Cornell, 2009). Vulnerability management is a security practice designed to prevent the exploitation of IT vulnerabilities that currently exist within an organization. The expected result is reducing time and money spent dealing with vulnerabilities and the exploitation of those vulnerabilities (Kabay et al, 2009). Proactively managing system vulnerabilities will reduce or eliminate the potential for exploitation and involve considerably less time and effort than responding after an exploitation has occurred (Kabay et al, 2009).

Security professionals usually use a tool to track and manage the status of known vulnerabilities, plus remediation/mitigation activities known as a vulnerability tracking and assessment system. The best-known example of such a system is the Defense Information Systems Agency (DISA) Vulnerability Management System –VMS (DISA, 2015). It is used to track and manage vulnerabilities throughout the United States Department of Defense (DoD). While VMS is a powerful tool for security professionals within DoD, it needs some improvements to better perform its roles. This paper will discuss the strengths and weaknesses of VMS as it exists and provides recommendations for the follow-on system, DISA's Continuous Monitoring & Risk Scoring (CMRS) system.

[1] My inspiration for this paper comes from the lessons drawn from several SANS Technology Institute classes. Namely, those classes include ISM 5100 (Enterprise Information Security), ISM 5300 (Building Security Awareness), and ISM 6000 (Standards Based Implementation of Security.)

John Dittmer, jdittmer@suprtek.com

2. Background

2.1 Early Development of Vulnerability Management Tools in General

During the early days of the Internet (late 1960s – early 1980s), most computer scientists never envisioned that users would use their network for destructive or illicit purposes (Timburg, 2015). Even though there were warnings such as a report from the 1970 DoD Science Board on potential computer vulnerabilities, most of the early developers thought Internet users would trust each other and act accordingly (Gamero-Garrido, 2013). Then, by the late 1980s, that view became quickly outdated. In 1985, a Soviet intelligence agent, Markus Hess, broke into several US military and research networks to gather intelligence on US military technology in the "Cuckoo's Egg" case (Gamero-Garrido, 2013). In 1988, malware such as the Morris worm were created and distributed wreaked havoc on computers and networks worldwide (Timburg, 2015). By 1990, many Western nations developed security standards for the governmental computers and networks. These standards usually included some sort of assessment process where Vulnerabilities become identified and assessed (Bishop, 2002).

In 1998, a young Frenchman, Renaud Deraison, developed the first widely used vulnerability assessment scanner called Nessus, which is still the most popular tool among security professionals (Piper, 2013). In 2002, he formed a company called Tenable with two partners. The next year, Tenable developed a management console for managing Nessus scans and their results (Piper, 2013).

However, there were still challenges for security professionals. Prior to 1999, information security tools that detected and/ or mitigated software security vulnerabilities had no way to interoperate with each other. There was no common means to identify or categorize

vulnerabilities (Piper, 2013). However, in 1999, that changed when MITRE Corporation — an American non-profit organization — compiled the first vulnerability database to assign a unique identifier to each vulnerability. MITRE's publicly available database – hosted by the U.S. National Vulnerability Database (NVD) at the National Institute of Standards and Technology (NIST) in partnership with MITRE — contains a unique common vulnerability and exposures identifier for each catalogued vulnerability (Piper, 2013). The identifier will be used in a variety of security tools such as vulnerability assessment and tracking tools (Piper, 2013).

2.2 Early Development of Vulnerability Management Tools within DoD

The early development of vulnerability management systems within DoD started in the early 1990s. Due to the classified nature of many of the information security-related projects performed by DoD, there are few public sources about the projects themselves. Therefore, I had to rely on a series of interviews with personnel that I had previously worked with as a contractor for DISA and the National Security Agency. Essentially, DISA and the National Security Agency have a long-standing agreement about the development of Information Security projects. The National Security Agency uses its vast network of laboratories and vendors to develop solutions, software, and other products as prototypes. Once the prototypes achieve a level of stability and maturity, then the National Security Agency will perform rigorous testing and additional development. Once both agencies agree that the project's deliverable has reached an acceptable level of maturity, the project is transferred over to DISA as a Program of Record for which that agency has the responsibility to operate and maintain (Frank, 2009). I had participated in such a project myself as a contractor in 2009-2010 when I had worked for Booz Allen Hamilton.

How this process described about relates to the development of vulnerability management systems was as follows. In the late 1980s and the early 1990s, security threats such malware and unauthorized hacking started to gain the attention of Information Security leaders in both industry and the government. It became apparent that solutions for disseminating and tracking information about vulnerabilities as well as remediation and mitigation activities had to be developed. At this point, Joint Task Force – Global Network Defense (later, Joint Task Force – Global Network Operations, the forerunner to today's US Cyber Command) had to rely on DISA using phone calls and emails to track compliance and reporting back on the status in the form of charts (Ruth, 2015). In 1995, DISA and the National Security Agency, with the help of other DoD Components (e.g. the military services and agencies) and supporting contractors, created the Vulnerability Compliance Tracking System (VCTS) (Snouffer, 1999). This system was a major step forward in that it provided DISA with the ability to quickly notify and receive acknowledgement from DoD Components of vulnerabilities (Snouffer, 1999). In addition, VCTS allowed users to assess the impact of vulnerability on the infrastructure. DISA could use VCTS to monitor the status and closure of vulnerabilities as well as provide reporting to DoD officials of compliance (Snouffer, 1999). These capabilities will be eventually incorporated into DISA VMS as well as early commercial solutions such as iDefense Vulnerability Contributor Program (now owned by Verisign) and Tipping Point Zero Day Initiative (now owned by Hewett Packard) (Zoller, 2011).

2.3 Historical Background of DISA VMS

DISA VMS can trace its historical origins from a widespread security attack. In February 1998, there was a series of attacks on over 500 computer networks, known collectively as Solar Sunrise (NIPC, 1999). Targets of the attacks included the DoD, American and Israeli universities, Internet Service Providers in the United States, Israel, and the United Arab

Emirates, as well as the Israeli Parliament, among other sites (NIPC, 1999). An Israeli hacker named Ehud Tenenbaum, working with two teenaged hackers from the United States performed these attacks (Sinai, 2008). In one of their exploits, the hackers exploited an e-mail and web server that was using an outdated version of Linux to gain access to user names and passwords, which they used to access other networks, since many people use the same user names and passwords for a variety of accounts (MIT News Office, 1999). The attacks coincided with a time of tension between the United States and Iraq over suspected weapons of mass destruction, which made it critical for American authorities to determine the origin of the attacks and put a stop to them (NIPC, 1999). Tenenbaum was later sentenced by an Israeli court to a year and half in prison (Sinai, 2008).

During this series of attacks, a known system vulnerability in the Solaris operating system was exploited even though the Joint Task Force – Global Network Defense had released a notice of the vulnerability and the required patch information (DISA, 2015). At the time, system administrators had to subscribe to a service to receive the bulletins. Recognizing that a subscription service was not sufficient, the Deputy Secretary of Defense, John Hambre, ordered the creation of the Information Assurance Vulnerability Management (IAVM) process (DISA, 2015). He required that vulnerability notices be sent through the command channels to all system administrators. Then, system administrators acknowledge receipt of that notice, apply changes to assets within 30 days, and perform period checks to monitor compliance (DISA, 2015). In addition, he charged DISA with collecting the required metrics from each Combatant Command, Service, and Agency, also known collectively as DoD Components. DISA created the IAVM web application to track these metrics as well as the receipt acknowledgement from each DoD Component. DISA, recognizing that collecting and monitoring the IAVM information could not

be done manually, created the Vulnerability Compliance Tracking System. This system was built for DISA but with open data architecture so that any DoD Component conducting an audit or review could utilize the VMS to track the status of findings from that review. The use of VCTS by DoD Components was optional, and Defense Department's enterprise funding supported the use of Vulnerability Compliance Tracking System across DoD. The IAVM and Vulnerability Compliance Tracking System web applications notified approximately 3,000 members of the command and security channels, as well as system and network administrators, of a vulnerability notice within minutes of issuance. Eventually, these systems were integrated to become VMS in its present form (DISA, 2015).

2.4 Description of the DISA VMS

VMS is a program operated by the DISA Field Security Office, based at the Letterkenny Army Depot in Chambersburg, Pennsylvania. It is the sub-component of DISA, which is responsible for enhancing security and availability of DoD networks by ensuring adherence to Information Assurance and NetOps Policies including development of guides and procedures. In addition, FSO conducts Information Assurance training of DoD Components; implementation of Enterprise Information Assurance solutions; formal certification reviews; vulnerability management tools and metrics; as well as support activities for Network Defense, Incident Response; and inspections (DISA, 2015).

In performing many of the functions listed above, the Field Security Office operates VMS. It assists all DoD Components in the identification of security vulnerabilities and tracks the issues through the lifecycle of the vulnerabilities existence. Streamlines automation of vulnerability tracking through a relational database and online web views that provide a centralized repository for vulnerability status information and policy compliance information for

both on clients with NIPRNet (a collection of DoD unclassified networks) and SIPRNet (a collection DoD classified networks at the SECRET level). VMS information is used for many purposes from practical vulnerability remediation to approval to operate (DISA, 2015).

The CNDSP Certification and Accreditation process started to utilize the VMS to record and track the findings associated with the CNDSP evaluations. The inspection processes also utilize the VMS to record and track findings. Security experts have recognized that systems implemented "out-of-the-box" do not have the proper configuration controls for known vulnerabilities. Personnel responsible for the administration and security of these systems are not restricted to ordering hardware and software from a specific vendor. Hardware can be ordered from various vendors (e.g., Gateway, Sun, Hewitt Packard, etc.) and a variety of operating systems (e.g., Windows, UNIX, Linux, etc.) and applications (e.g. Microsoft, Oracle, command legacy, etc.) can be installed on the aforementioned hardware and operating systems in various permutations. Through the combination of improper configuration, the process of aging, and the addition of third-party software, these systems can fall out of compliance with DoD security policies and become vulnerable to attack. The Security Readiness Review process seeks to identify those vulnerabilities and track them through closure and validation. Due to the wide and increasing proliferation of vulnerability scanning tools, VMS will be more interactive and support automated interfaces for near real-time data loading. Examples of these scanning tools include the Assured Configuration Assessment Solution (ACAS - a modified version of Nessus), eEye's Retina, Internet Security System's scanning tool, etc. These interfaces will include authentication, compression, encryption, asset registration and unique asset identification. Any approved scanning tool can be used to report findings to VMS so long as the output conforms to the extensible markup language definition, and the vulnerabilities match those listed within

VMS. Perhaps one of the largest issues that local System Administrators have is how to securely administer a centrally managed program. VMS seeks to bridge that gap by providing Program Managers with the ability to post action plans for both known and emerging vulnerabilities, seek mitigation approval from the program Designated Approving Authority (the DoD equivalent to a Chief Information Security Officer), and communicate all of these actions to the System Administrators administering their systems (DISA, 2015). The Designated Approving Authority is the senior DoD official with the authority to form assume responsibility for operating a system at an acceptable level of risk (DoD CIO, 2014).

DISA had the VMS architecture built with the vision to integrate the systems into one common platform, allowing a comprehensive system to determine the posture of an organization's infrastructure. A single, common platform will also enable a Designated Approving Authority to assess risk during accreditation activities across programs and systems for all types of vulnerabilities. The addition of the CNDSP Certification and Accreditation information will also assist organizations with understanding the CND capabilities of organizations (DISA, 2015).

The DISA brochure on VMS describes the system as an Information Assurance tool that provides services broken down by VMS Capability Areas, which include the following functions to support DoD activities (DISA 2015). First, VMS provides for the registration and management of network assets (both computing and non-computing), programs, systems, and enclaves. Second, the system provides vulnerability finding maintenance. To do this, VMS allow users to conduct vulnerability tracking and create a record of compliance that is known as a Plan of Action and Milestones. Second, the system provides a repository for audit and

inspection results & training. Finally, VMS is used for issuing notices such as vulnerability alerts, tasking orders, warning orders, and other DoD mandated directives) (DISA, 2015).

VMS is capable of performing these functions because of the existence of the Security Content Automation Protocol (SCAP). SCAP is a synthesis of interoperable specifications that permits data flows between a variety of Information Assurance tools. The protocol is being incorporated in a number of Information Assurance tools under development (Decker, 2011). With SCAP, DISA can take information from the NVD to populate VMS with information on vulnerabilities. The NVD is a national repository of information regarding vulnerabilities. Integrating NVD and VMS CND is a Defense in Depth integrated approach to the management of enterprise information assurance. VMS contains DOD-only SCAP data and DOD SCAP compliance data. DISA will have VMS will publish DOD-related SCAP back to the NVD as it deems appropriate (Mell & Inverso, 2008).

3. An Assessment of the Strengths and Weaknesses of the DISA VMS

3.1 Strengths

The following is a summary of the strengths of DISA VMS based on a variety of conversations and briefings I had while I was a contractor supporting the DoD Computer Network Architect (a member of the DoD Chief Information Officer's staff) from 2009 - 2012.

- Provides DoD with in-depth information about the security posture of its networks.
- Provides senior leadership with Plans of Actions and Milestones to show what system owners are doing to remediate/mitigate vulnerabilities. This includes estimated times to remediated with milestones.

- Helps to expedite the timely resolution of vulnerabilities
- Disseminates vulnerability notifications (DISA, 2015)
- Tracks assets
- Tracks the receipt of vulnerability notifications and their compliance
- Manages plan of action and milestones
- Provides system administrators with security guidance
- Integration with scanning tools (DISA, 2015)
- Near real-time updates (DISA, 2105).

3.2 Weaknesses

The following is a summary of the weaknesses of VMS based on a variety of conversations and briefings during my time with the DoD Chief Information Officer's staff. In addition, other users and I discovered some of these weaknesses during VMS regarding Office of Naval Research's remediation efforts for the vulnerabilities found during the November 2014 Navy Cyber Security Inspection. These suspected weaknesses were confirmed in briefings hat were discovered research on the subject. First, current DoD systems, such as VMS for tracking vulnerability compliance, are siloed and lack standard interfaces (Distefano & Wolfkiel, 2014). Even DISA stated this as fact in their briefings on the introduction of CMRS (Decker, 2011). The information on VMS is based on inputs from the commands that could be false or misleading. Inputting data manually is a long, slow process (Decker, 2011). This is especially true on the SIPRNet, where encryption sometimes takes up a lot of bandwidth. It is often hard to find individual vulnerabilities since they are sometimes not in alphanumerical order for some assets. In addition, the search feature does not work well.

3.3 The Future of VMS

In October and November 2014, the DISA Project Manager for CMRS, Scott Distefano, along with the DISA Leader Engineer for the Secure Configuration Management Architecture, Joseph Wolfkiel, presented two briefings to the DoD Community of Interest on the future of VMS and the introduction of CMRS. They said that by 2016, all of the VMS system functions must evolve to new processes or be transitioned to one of the following options: 1) the Digital Policy Management System; 2) CMRS; 3) Enterprise Mission Assurance Support Service which is used heavily for certification and accreditation of DoD systems; 4) CMRS & Enterprise Mission Assurance Support Service Integration at a future date (Distefano and Wolfkiel, 2014).

The transition goals are to increase automation for the monitoring of vulnerabilities, minimize self-reporting, validate of secure configurations, and increase the level network security. In addition, there is also the goal to provide a technical foundation to facilitate and support the transitions to the Risk Management Framework and Information Security Continuous Monitoring (ISCM) (NIST, n.d.).

4. An Introduction to the DoD Continuous Monitoring and Risk Scoring (CMRS) System

4.1 Historical Background

Following up the publication of the 20 Critical Controls, the U.S. Department of State validated the consensus controls in 2009 by determining whether the controls covered the 3,085 attacks it had experienced in Fiscal Year 2009 during the period between 10/01/2008 – 09/30/2009 (Distefano & Wolfkiel, 2014). In a presentation to the Intelligence Community, the State Department's Chief Information Security Officer, John Streufert, reported remarkable alignment between the consensus controls and the actual attacks experienced by the State

Department (SANS, n.d., *Critical Security Controls: A Brief History*). He also launched a program to implement automated capabilities to enforce the key controls and provide daily mitigation status information to every system administrator across 24 time zones in which the State Department operates. This marked the beginning of the movement towards Continuous Monitoring within the United States Federal Government rather than relying on periodic certification and accreditation processes. These processes provide a snapshot of the status of information security at a point in time. Having rapidly achieved a reduction of more than 88% in vulnerability-based risks across 85,000 systems, the State Department's program became a model for large government and private sector organizations. In December of 2011, then Secretary of Homeland Security Janet Napolitano appointed John Streufert as the Director of the National Cybersecurity Division, with the mandate to bring about the same type and level of risk reduction across the government and its critical infrastructure as he had done at the State Department (SANS, n.d., *Critical Security Controls: A Brief History*). During this period, the Department of Defense, started to ramp up similar projects, especially within the Army with its pilot program. DISA is in the process of expanding the system to cover all of DoD's networks (Distefano & Wolfkiel, 2014).

4.2 CMRS System Description

CMRS is intended to be the DoD's enterprise-wide tracking system for network assets with an initial focus on collecting and providing information related to - Enterprise hardware and software inventories for networked devices on NIPRNet and SIPRNet. Compliance with enterprise mandates are packaged as "benchmarks" and compliance with mandates to deploy common defense-in-depth mitigation tools. Operational context information required for rollup

and drilldown of data, and command and access control. It is DISA's intention that risk associated with findings will drive remediations and mitigations (Distefano & Wolfkiel, 2014).

For users, CMRS tracks the following metrics in regards to systems within their accreditation boundaries (or systems under their responsibility):

- Inventory – What assets does one have, how are they are configured and where are they deployed? The reason why this is important is that often vulnerabilities lie in systems or devices that system administrators did not even know was on their networks. These metrics are related to Critical Security Controls 1, 2, and 3 (SANS. (n.d.) *Critical Security Controls for Effective Cyber Defense).*
- Compliance – What are the capabilities of the command's assets and how are they configured? How are they supposed to be (in compliance with DoD standards)? What are their weaknesses? This is significant because ignorance of the capabilities of network assets and their capabilities can lead to the creation of vulnerabilities or allow them to remain hidden. These metrics are related to Critical Security Controls 3 and 10 (SANS, (n.d.) *Critical Security Controls for Effective Cyber Defense).*
- Owning and Administering Organization – Who is responsible for fixing them? Who is responsible for defending them? Often vulnerabilities are not remediated or network defenses are weakened due to unclear roles and responsibilities (Distefano & Wolfkiel, 2014).
- Mission Dependence – What mission do my assets support? Based on inventory, compliance, what missions are at risk to compromise in availability, confidentiality, and integrity? Often vulnerabilities go not remediated or network defenses are weakened due to unclear roles and responsibilities. Within the DoD, the type of mission often define

which security controls need to be in place for a system or network (Distefano & Wolfkiel, 2014).

- Risk – What should be fixed first or allocate resources to actively defend. Battle Damage Assessment – If successfully attacked - what have is lost or compromised, how can it be fixed, and how critical is that to mission success? These questions are essential for network defense (Distefano & Wolfkiel, 2014).

During their briefing, Distefano & Wolfkiel maintained that in order to obtain the data for the metrics listed above; CMRS uses the following systems or modules such as the Host Based Security System that provides information on managed devices operating systems, Mission Assurance Codes, Internet Protocol addresses, and hostnames. In addition, there are installed endpoint products, and Host-based Intrusion Prevention Systems and Anti-Virus data file dates & versions. A service that CMRS provides is Rogue System Detection for unmanaged devices. The Operation Attribute Module displays operational attributes owning, administrating, and defending organizations. The Policy Auditor module produces security benchmark results for compliance with IAVMs and Security Technical Implementation Guides. The Asset Configuration Compliance Module checks for the installed Operation System, software, and patches. At this point, ACAS is feeding information into the Host Based Security Service. Vulnerability scan results demonstrate compliance with policies, IAVM notices, and secure configuration guidelines (Distefano & Wolfkiel, 2014). Some DoD Components are using Tenable's Security Center management console to run the ACAS scans and report results. Security Center is operated by DISA as a service to make the transition easier (Distefano & Wolfkiel, 2014).

The other part of CMRS, Risk Scoring, is done by asset count vs. open findings. The scoring mechanism for areas of compliance is split into various statistical "buckets":

- Antivirus Reporting
- Antivirus Compliance
- Host Based Security Service Reporting
- Host Based Security Service Compliance
- IAVM Reporting
- IAVM Compliance
- Operating System Security Technical Implementation Guide Reporting (Distefano & Wolfkiel, 2014).

The security management theory behind using these metrics in risk scoring is that the scores indicate to senior managers where they need to focus resources and efforts for remediation and mitigation of vulnerabilities.

4.3 CMRS Future Capabilities

In their briefing, Distefano and Wolfkiel (2014) described the following future capabilities of CMRS:

- CMRS will include inventory and scoring of mobile devices, compliance with the Federal Information System Management Act, and network devices. DISA is in the process of providing secure mobile devices throughout DoD, so controlling the inventory and ensuring their secure configuration is becoming a priority.
- CMRS will be adding scoring from other sensors such as Big Fix, Blade Logic, etc.

- DISA will be developing Enhanced User Interfaces and enhanced data tag support to provide more ways to view the data and more intuitive screens. This will be helpful as security personnel may need to view security related data in new ways to might future threats.
- As the Defense Department adopts the by Risk Management Framework security controls from NIST, CMRS will provide more roll-up and drill-down capabilities in viewing security controls in its interface.
- CMRS will identify Cyber Command Readiness Inspection requirements and include scoring for compliance and implementation of remediation of vulnerabilities.
- Support the transition of VMS capabilities to newer systems (NIST, 2012).

Hopefully, that these innovations will make CMRS more flexible in assisting DoD Information Assurance personnel gain an understanding of the security status of their systems. This way, they can better implement security initiatives such as the Critical Security Controls.

5.0 Conclusion: Recommendations for CMRS Future Capabilities

While CRMS will provide enhanced capabilities for vulnerability management within DoD, there is still room for future improvement. Most of my recommendations concern those systems provide information regarding vulnerability management to the system.

Based on research, any vulnerability management system should be capable of providing information and supporting the following processes:

- Vulnerabilities become identified
- Vulnerabilities are assessed
- Vulnerabilities are classified

- Vulnerabilities are tracked
- Vulnerabilities are managed
- Vulnerabilities are resolved (Piper, 2013)

Based on the processes, listed above the first recommendation would be to provide a data feed from the NVD repository of information on vulnerabilities. Part of that repository includes a risk score on vulnerabilities, which is quite useful in setting priorities on which vulnerabilities to remediate first (Distefano & Wolfkiel, 2014). The risk scores are also useful in creating Plans of Actions and Milestones. Currently, when scans on systems are performed using the ACAS tool and security personnel are reviewing the results, they have to manually go into the NVD and determine what the risk scores are (Distefano & Wolfkiel, 2014). It would be useful if the ACAS tool has an interface with the NVD so it can automatically provide the risk score for the vulnerabilities in reports. In turn, users can those reports fed directly into CMRS, thus saving a few work steps.

The second recommendation concerns how commands and agencies prepare for inspections and evaluations. Currently, preparing for inspections is a difficult and labor-intensive process. In my experience as an Information Assurance Team Lead who successful passed the Navy's version of the Command Cybersecurity Readiness Inspection, there is some guesswork involved. System engineers and security personnel go through security documentation such as the Security Technical Implementation Guides which described how proper how to set up systems and devices to be properly configured. However, there is a fair amount of guesswork on to interpret the Security Technical Implementation Guides. It would save a lot of guesswork if system engineers and security personnel can run automated scans of their systems and devices from CMRS much as if they can run scans to see if they comply with

IAVMs and Cybersecurity Task Orders. Then, work on systems can be more focused on remediating vulnerabilities that are discovered ahead of the inspection rather than trying to catch up afterwards.

If incorporated, these suggestions will help future versions of CMRS to improve the security of DoD networks while freeing up resources for its Information Assurance personnel.

John Dittmer, jdittmer@suprtek.com

References

Bishop, M. (2002). Computer Security: Art and science (p. 938). Boston, MA: Addison-Wesley.

Chabrow, E. (2012). State Department's Streufert Moves to DHS. *Gov Info Security*. Retrieved April 16, 2015, from: http://www.govinfosecurity.com/state departments-streufert-moves-to-dhs-a-4405.

Cornell, D. (2009). Vulnerability Management in an Application Security World. *Denim Group Blog.* Retrieved April 19, 2015, from: http://www.denimgroup.com/media/pdfs/VulnerabilityManagementInAnApplicaitonSecurityWorld_OWASPSanAntonio_20090129.pdf.

Decker, G. (2011). DoD's NexGen Vulnerability Management on the Road to Full Automation. Retrieved April 4, 2015 from: http//scap.nist.gov/events/2011/itsac/presentations/day3/Decker-NexGen Vulnerability Management.pdf.

Department of Defense Chief Information Officer (DoD CIO). (2014) DoD Instruction 8500.01: *Cybersecurity.* Retrieved May 5, 2015 from: http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf

Distefano, S., & Wolfkiel, J. (2014). NIST & DISA joint briefing. *Continuous Monitoring and Risk Scoring (CMRS) 2.0 End to End*, *Parts I & II.*

DISA VMS Information Brochure. Retrieved April 3, 2015 from: https://disa.deps.mil/ext/cop//iase/vms.

Frank, L. (2009, April 10). Discussion on DISA and NSA Collaboration [Personal interview]. Note: Mr. Frank is a retired US Army Colonel who the first Assistant Commander for Operations of the Joint Task Force – Computer Network Defense. He was my manager at Booz Allen Hamilton who was preparing me for working the Deputy Program

Manager on a joint National Security Agency – DISA project for the next generation IAVM system.

Gamero-Garrido, A. (2013, December 1). Cyber Conflicts in International Relations: Framework and Case Studies. Retrieved June 3, 2015, from http://ecir.mit.edu/images/stories/Gamero_Case studies in Cyber Conflict_Final.pdf

Government Accounting Office – GAO. (2011). *Defense Department Cyber Efforts: DoD Faces Challenges in Its Cyber Activities (GAO-11-75).* Retrieved May 3, 2015 from http://www/gao.gov/new.items/d1175.pdf.

Jones, S. (2015, May 26). Discussion about early VMS Research [E-mail interview]. Note: Ms. Jones is a Program Manager at the National Security Agency.

Kabay, M., Whyne, E., & Bosworth, S. (2009). *Computer Security Handbook (5th ed.).* Hoboken, NJ: John Wiley & Sons.

Mell, P. & Inverso, P. (2008). NIST and DISA SCAP briefing. Retrieved April4, 2015 from https://nvd.nist.gov/scap/docs/2008-conf-presentations/day1/nvd-vms-scap-integration-v7.pdf.

Massachusetts Institute of Technology (MIT) News Office. (1998). Two boys in California Break into PSFC Computer. *MIT Tech Talk.* Retrieved April 4, 2015 from: http://web.mit.edu/newsoffice/tt/1998/mar04/hack.html.

National Infrastructure Protection Center (NIPC). (1999). Solar *Sunrise: Dawn of a New Threat (NIPC Training Video).* Retrieved May 5, 2015 from: https://www.youtube.com/watch?v=bOr5CtqYnsA

National Institute of Science and Technology (NIST). (2012). *Guide for Conducting Risk Assessments*. Special Publication 800-30, Rev I. Retrieved April 5, 2015, from: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

National Institute for Science and Technology (NIST). (2015). *Security Content Automation Protocol* (SCAP). Retrieved April 1, 2015 from: http://scap.nist.gov/index.html.

Piper, S. (2013). Understanding Vulnerability Management. In Definite Guide to Next-Generation Vulnerability Management (pp. 3-9). Annapolis, MD.

Ruth, D. (2015, June 2). Discussion of the Origins of VMS [E-mail interview]. Please note: Professor Ruth is the DISA Visiting Professor at National Defense University.

SANS. (n.d.). *Critical Security Controls: A Brief History*. Retrieved March 31, 2015 from: http://www.sans.org/critical-security-controls/history

SANS. (n.d.). *Critical Security Controls for Effective Cyber Defense.* Retrieved March 31, 2015, from http://www.sans.org/critical-security-controls.

Sinai, Liron. (2008). *Canada: Israeli Hacker Suspected of Involvement in Major Fraud Case.* Retrieved May 15, 2015, from http://www.ynetnews.com/articles/0,7340,L-3592642,00.html

Snouffer, J. (1999, February 9). Information Assurance Vulnerability Alert DISA Internal. *Briefing at the Defense information Systems Agency*. Lecture conducted from Defense Technical Information Center, Falls Church, VA. Retrieved May 28, 2015, from: http://www.dtic.mil/dtic/tr/fulltext/u2/a390651.pdf.

Timberg, C. (2015, May 30). Net of Insecurity: The Making of a Vulnerable Internet. The Washington Post. Retrieved June 3, 2015, from http://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/.

John Dittmer, jdittmer@suprtek.com

Zoller, T. (2011, December 1). The Rise of Vulnerability Markets - History, Impacts, Mitigations. *Open Web Application Security Project - BENELUX Day*. Lecture conducted from Open Web Application Security Project, Luxembourg City, Luxembourg.

List of Abbreviations

ACAS - Assured Configuration Assessment Solution

CIO - Chief Information Security Officer

CMRS - Continuous Monitoring and Risk Scoring

CNDSP – Computer Network Defense Service Provider

DISA – Defense Information Systems Agency

DoD – Department of Defense

DHS – Department of Homeland Security

GAO – Government Accountability Office

IAVM – Information Assurance Vulnerability Management

MIT – Massachusetts Institute of Technology

NIPC – National Infrastructure Protection Center

NIST – National Institute Standards and Technology

NVD – National Vulnerability

SCAP – Security Content Automation Protocol

VMS – Vulnerability Management System

John Dittmer, jdittmer@suprtek.com

Last Updated: October 20th, 2017

Upcoming SANS Training

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

SANS San Diego 2017	San Diego, CAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, AE	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Milan November 2017	Milan, IT	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Amsterdam 2017	Amsterdam, NL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Miami 2017	Miami, FLUS	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Paris November 2017	Paris, FR	Nov 13, 2017 - Nov 18, 2017	Live Event
Pen Test Hackfest Summit & Training 2017	Bethesda, MDUS	Nov 13, 2017 - Nov 20, 2017	Live Event
SANS Sydney 2017	Sydney, AU	Nov 13, 2017 - Nov 25, 2017	Live Event
GridEx IV 2017	Online,	Nov 15, 2017 - Nov 16, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CAUS	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, GB	Nov 27, 2017 - Dec 02, 2017	Live Event
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZUS	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Khobar 2017	Khobar, SA	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TXUS	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, DE	Dec 04, 2017 - Dec 09, 2017	Live Event
European Security Awareness Summit & Training 2017	London, GB	Dec 04, 2017 - Dec 07, 2017	Live Event
SANS Bangalore 2017	Bangalore, IN	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Frankfurt 2017	Frankfurt, DE	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DCUS	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS SEC460: Enterprise Threat Beta	San Diego, CAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Berlin 2017	OnlineDE	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced