IT Security support for the Spaceport Command & Control System Development Ground Support Development & Operations

Drew Branch

Kennedy Space Center

July 11, 2014

Author Note

Drew A. Branch

B.S. in Electrical and Computer Engineering, *Morgan State University*

M.P.S. Cybersecurity, *University of Maryland, Baltimore County* (In Progress)

Contact: DrewBranch@umbc.edu

Table of Contents

Abstract

Security is one of the most if not the most important areas today. After the several attacks on the United States, security everywhere has heightened from airports to the communication among the military branches legionnaires. With advanced persistent threats (APT's) on the rise following Stuxnet, government branches and agencies are required, more than ever, to follow several standards, policies and procedures to reduce the likelihood of a breach. Attack vectors today are very advanced and are going to continue to get more and more advanced as security controls advance. This creates a need for networks and systems to be in an updated and secured state in a launch control system environment.

FISMA is a law that is mandated by the government to follow when government agencies secure networks and devices. My role on this project is to ensure network devices and systems are in compliance with NIST, as outlined in FISMA. I will achieve this by providing assistance with security plan documentation and collection, system hardware and software inventory, malicious code and malware scanning, and configuration of network devices i.e. routers and IDS's/IPS's. In addition, I will be completing security assessments on software and hardware, vulnerability assessments and reporting, and conducting patch management and risk assessments. A guideline that will help with compliance with NIST is the SANS Top 20 Critical Controls. SANS Top 20 Critical Controls as well as numerous security tools, security software and the conduction of research will be used to successfully complete the tasks given to me. This will ensure compliance with FISMA and NIST, secure systems and a secured network. By the end of this project, I hope to have carried out the tasks stated above as well as gain an immense knowledge about compliance, security tools, networks and network devices, as well as policies and procedures.

Project Description

I provided IT support to Spaceport Command & Control System Development Ground Support Development & Operations. The majority of my projects were geared towards ensuring that the networks, as well as the network devices and workstations are in compliance with FISMA and NIST 800-53. The department went through the initial phase of an audit to either confirm or deny compliance and it is imperative that the audit is passed. The networks and devices must be secure because communication cannot be lost between the people on the ground and computer systems and/or astronauts in the air because of a breach in security. During this session, projects given to me had a direct correlation in the compliance efforts.

COTS Software

One of my first projects that I was given was to gather information about various commercial off-the shelf (COTS) software. These software solutions were user tested, vetted and will help with compliance with NIST 800-53 rev 4. I called numerous vendors to gain information about their products' capabilities and how they can be implemented in our environment. For me to complete this, I had to understand the network and devices on the network and what they are used for. I gathered quotes from companies where the software solutions: fulfilled the NIST compliance requirement, supported end user systems and network devices and did not impact performance of systems drastically.

SANS Top 20 Critical Controls

The SANS Institute put together a Top 20 Critical Controls guideline to help organizations fulfill their NIST compliance requirement. This guideline was used to make compliance with NIST more manageable. I was given the task to familiarize myself with each critical control and understand why they are critical and the relationship with NIST 800-53. I updated an interactive spreadsheet with current information regarding the SANS Top 20 Critical Controls and with the newest version of NIST 800-53 correlations. This spreadsheet is the core document being used to determine if the solutions implemented now will still fulfill the compliance requirements of the new revision of the NIST 800-53 document.

Project Management Tools

Project management is key to the success of any project. If a project management scheme is executed correctly it can reduce project cost, keep tasks on schedule with corresponding deadlines, and produce the planned outcome of the product. I found a project management web based tool that helped with organizing tasks, keeping track of deadlines, and gave ability for group members to communicate with each other in a forum environment. I also gave a briefing about this product to various group members on how to use it and its capabilities.

Secure Software Recommendation Assessment

A company who specializes in secure programming techniques was up for contract consideration. Two other interns and I completed an assessment on their service and techniques. After conducting extensive research, we found that the company was in compliance with the SANS Institute and made a good curriculum to teach programmers

how to program secure software. Within the assessment, we were required to give a recommendation. The company took bits and pieces from various well-known sources and made it their own. The benefit of the company was that they would teach the programmers instead of having them teach themselves. Our recommendation was that the company offered a great service and was convenient and depending on the price, it was a go.

Penetration Testing Tool Analysis

Every network and/or organization should go through the penetration testing process. This process exposes the vulnerabilities within your network and can also expose vulnerable people who are susceptible to social engineering attacks. I was given the task of testing a penetration device, documenting its capabilities, and to create a how to guide and present my findings. Testing this penetration box was very intriguing. Its capabilities were far more than what it was bought for. The purpose of this device was to be set up remotely and scan for unauthorized wireless networks at KSC. Since the penetration device had many features, after I tested its capabilities for wireless network scanning I was given the chance to explore more. I found that this device not only can scan for wireless networks but can also try to hack into them, record network traffic, scan for vulnerabilities on systems and possible compromised a systems using Metasploit to do so. This device is a sheevaplug, which means it's a computer in a box. This device ran a version of the Linux operating system and can be accessed through a Backtrack, Linux distribution. I sent commands to this device by setting up a SSH connection via a Kali Linux machine.

Risk Automation

Risk automation is key to identify the risks of the systems on the network. This takes out the need to physically audit each machine. The software that I used has a vast number of features and capabilities such as: port analysis, vulnerability assessment, and system information to name a few. This software was used to scan and identity systems that had unused software on them. After they were identified, a number of reports were created for the different computer systems according to the operating system the system was running. These reports were forwarded to the IT department, who are in charge of imaging workstations, servers, etc.

Anti-Virus Product Research and Testing

There are a plethora of viruses, malware, rootkits and Trojans out in the world today. Anti-virus software is a key component to securing systems from the devastating consequences that might arise with an infected system. I researched and tested several anti-virus products that were in compliance with NIST and FISMA. I was a key part in the selection process because I created documents and produced artifacts that narrowed down the list dramatically and management ultimately selected the product that I thought was the best.

Active Directory Solution

An active directory solution was needed for UNIX based systems to connect to the NASA network using the employees' credentials. This was critical because having a solution that enabled cut costs and freed up employee resources. If this would have been done manually by an employee, an active directory would have to be created and monitored for

all users. I supplied a couple of solutions with corresponding quotes that would enable this action.

Security Monitoring Center

I was given the task to research, test and install a security monitoring center product. The selected product had to monitor networked devices such as routers, switches, workstations and firewalls. The solution also had to generate compliance reports and have the capability to email certain responsible parties when something when an incident happened along with other requirements as stated in the NIST 800-53 compliance document. This product was first introduced into a sandbox test bed after testing for a month, the solution did everything that was needed and the procurement process was started. After the purchase of the product it was deployed in the development environment for further testing in a real life environment.

Beneficial Exposure

Currently, I am completing my master's degree in cybersecurity at UMBC. The program that I am enrolled in is geared more towards government IT security, law and policies. Fortunately for me, this internship has a direct correlation with what I learned before coming to the Kennedy Space Center and what I will build on further when I leave. So far, this experience is great and I will definitely take this experience and everything I learned while at KSC with me in my future.

This opportunity enhanced already possessed skills, exposed me to new skills and provided hands on experience with software and hardware that I will use in my career field. My communication skills, confidence in public speaking, and knowledge about numerous IT security subject matters are being built by going to group meetings and

actively expressing myself within them. Also by me receiving real work, I am gaining real world IT security experience. In graduate school I learned about: mitigation, risk analysis, policy making, business continuity plans, disaster recovery plans, network devices, attack vectors, compliance laws, patch management, and various other security tools. By being here, I am gaining a real world, in-depth experience on all of those topics and how they are implemented and sustained.

This opportunity is a perfect opportunity for me. I am doing work that interests me, that is relevant to current security topics and I am gaining experience that employers are looking for in a future employee. I am convinced that after my yearlong internship I will have a considerable advantage over the average graduates competing for the same job. This is due to the fact that I am getting a complete experience of the IT security field and IT security insight from a government aspect.

Conclusion

To date, I have gained valuable knowledge and experience. So far, I have worked on compliance projects, a project management project, carried out a secure programing service analysis and assessment, analyzed security issues using risk automation software, and completed a penetration device testing and assessment. Also, I gained valuable non-technical skills dealing with budget requirements and making decisions for products that satisfies the most security requirements. I have been involved in many different facets of IT security and I have only completed about thirty-three percent of my internship. This experience is the highlight of my career so far. I am extremely excited to return to KSC for my next session, to get new relevant projects and expand my experience and knowledge.