IT Security support for the Spaceport Command & Control System Development.

Brian Varise
NASA Kennedy Space Center
Major: Computer Science
KSC-FO Summer Semester
11 July 2014

Table of Contents

Abstract

My job title is IT Security support for the Spaceport Command & Control System Development. As a cyber-security analyst it is my job to ensure NASA's information stays safe from cyber threats, such as, viruses, malware and denial-of-service attacks by establishing and enforcing system access controls. Security is very important in the world of technology and it is used everywhere from personal computers to giant networks ran by Government agencies worldwide. Without constant monitoring analysis, businesses, public organizations and government agencies are vulnerable to potential harmful infiltration of their computer information system. It is my responsibility to ensure authorized access by examining improper access, reporting violations, revoke access, monitor information request by new programming and recommend improvements.

My department oversees the Launch Control System and networks. An audit will be conducted for the LCS based on compliance with the Federal Information Security Management Act (FISMA) and The National Institute of Standards and Technology (NIST). I recently finished analyzing the SANS top 20 critical controls to give cost effective recommendations on various software and hardware products for compliance. Upon my completion of this internship, I will have successfully completed my duties as well as gain knowledge that will be helpful to my career in the future as a Cyber Security Analyst.

Job Description

I am a computer programmer but my job here at KSC is to provide IT Security support for the Spaceport Command, Control System Development, Ground Support Development and Operations (GSDO). I have been tasked by my mentor, Robert Van Arsdalen, to complete numerous projects dealing with IT Security. I plan and implement security measures to protect computer systems, networks and data. I am expected to stay up-to-date on the latest Security Software, as well as learn hacker's methodologies in order to anticipate security breaches. I am also responsible for preventing data loss and service interruptions by researching new technologies that will effectively protect a network. It is vital that the networks are secure so that communication does not get lost between users.

Projects

SANS Top 20 Critical Controls

My first project was to research and collect data from the SANS top 20 Critical Security Controls to give cost effective recommendations on different hardware and software products for acquiescence. The controls help the user master specific, proven techniques and tools needed to implement and audit the Twenty Critical Security Controls. The Top 20 Security Controls are rapidly becoming accepted as the highest priority list of what must be done and proven before anything else at nearly all serious and sensitive organizations. My mentor gave me this task to learn about the critical controls and know the importance of why it is used to stop potential cyber-attacks. The interns and I updated a shared spreadsheet with the current information about the SANS Top 20 Critical Controls and also added the latest version of NIST

800-53 correlations. Without using this spreadsheet, it would be hard to determine if the software that was previously installed will still fulfill the compliance requirements of the new revision of the NIST 800-53 document.

Penetration Testing

A penetration test is a process of assessing a computer's network security by mimicking an attack on a computer system or network from external and internal threats. The process involves an active analysis of the system for any possible vulnerabilities that could be cause from poor or improper system configuration, both known and unknown hardware or software flaws, and operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker and can involve active exploitation of security vulnerabilities.

A penetration test should be done on every company's networks to ensure that the network is safe from hackers. Running this test will allow users to explore the vulnerabilities inside the network and can also expose vulnerable people who are prone to attacks. Drew Branch and I were tasked to test a penetration device, researching all of its capabilities, and created a how to guide to present to members of the security team. The testing process of the penetration box was very fascinating. This device is a sheevaplug, it could do everything that a PC could do. The only thing it does not have is camera capabilities. We noticed that this device not only searches for wireless networks but it could also hack into them as well. This device can only be ran on Linux devices.

Commercial Off the Shelf Software (COTS)

I was given this project to collect data from numerous off the shelf (COTS) software. For about two months, Drew and I called about two hundred vendors to gather information about their featured products and how they can help improve the security in our department's network. I spent hours on the phone with sales representatives gathering information and also attending over twenty-five web demos to see how the products work.

I received many quotes from the vendors that that were cooperative and from there created a spreadsheet to give to the rest of the security team so that we can get together and decide which product would be the best fit for the department. In order for me to successfully finish this project, I had to learn the ins and outs of the networks and devices so that I would not choose a product that would not run properly on the networks in our department.

Risk Automation Suite

Risk Automation Suite (RAS) capabilities relate directly to the objectives of the National Institute of Standards and Technology (NIST) Secure Content Automation Protocol (SCAP), a method for using specific standards to enable automated and integrated vulnerability management, measurement and policy compliance evaluation. RAS Suite is the leading fully SCAP-validated enterprise class solution that provides accurate, continuous and automated IT risk metrics. Risk automation is key to finding the vulnerabilities of a network. Many users prefer to use the RAS because they won't have to audit each machine physically. This software has a huge number of capabilities and features such as: vulnerability assessment and port

analysis. The software scanned and identified systems that had vacant software on them. Once the software recognized, a list of reports were generated for the computer systems according to the system that was running the operating systems. When the reports were finished, they were sent to the IT department.

SCAP Report

The Security Content Automation Protocol (SCAP) is a method for automating the definition, consumption, and assessment of system configurations on desktop systems throughout an organization's infrastructure. SCAP consists of a suite of standards that enable automated vulnerability management, measurement, and policy compliance evaluation, for example, FISMA compliance.SCAP standards addresses objects such as enumerates software flaws, security-related configuration issues, and product names. Also measure systems to determine the presence of vulnerabilities. SCAP provides mechanisms to rank the results of these measurements to evaluate the impact of the discovered security issues. SCAP defines how these standards are combined. The U.S. National Institute of Standards and

Technology (NIST) maintains the National Checklist Program (NCP) and provides a repository of data feeds that use the SCAP standards. It is also the repository for official SCAP standards data. NIST defines and maintains the protocol and the data feeds of content in the SCAP standards. Thus, NIST defines how to use the open standards within the SCAP context and defines the mappings between the SCAP enumeration standards.

Sophos Endpoint Anitvirus

The Endpoint Antivirus security labs find more than 250,000 different threats everyday shielding laptops, desktops, and any devices connected to them from todays most advanced threats. 90% of threat can be prevented with a single patch. Sophos Endpoint Antivirus scans, identifies, and prioritizes critical patches from popular vendors such as Java, Adobe, Microsoft, and Apple. All emails are scanned for virus, spyware, Trojan horse, Malware, and Phishing. It also has integrated advance web threat protection to protect users from malicious websites and to block inappropriate content from entering the network. Managing the antivirus security settings and policies for every computer in a network can be done from a single console. The setup can be done remotely. It also has coverage for every platform.

Experience

Currently, I am completing Bachelor's degree in computer science at Alabama A&M University. Although, I do not learn anything about IT security at my university, I believe it will be very beneficial to my career in Engineering. This internship gives me a chance to work in a different field of computer engineering and by learning this, it will help me become a more diverse engineer. This has been a great experience for me working at Kennedy Space Center and I will certainly utilize everything that I have learned here in the future when I begin my career at a computer engineer.

This internship opportunity has allowed me to learn new skills and receive hands on training with hardware and software in the field of IT Security. It also enhanced my

communication and computer skills. Doing real world work is giving me the full experience I will need in order to be a successful IT security analyst in the future. I began to become confident in speaking publically and improved my knowledge about IT security. The group meetings helped me understand the importance of teamwork and delegacy. Without working together as a team, nothing would get accomplished right. This is a great opportunity for my family and I. I enjoy being part of a team that has the potential to change the world.

Conclusion

I am very excited to be an intern at KSC. Ever since I was a kid I've always wanted to work for NASA. I have received lots of important information and experience. I have met a lot of helpful people during my KSC experience. They would always tell me to make sure I soak up all of the information that I am learning here and utilize it when I start my career. They also taught me the importance of hard work. Working here at KSC has shown that anything is possible if I put my mind to it. My mentor Rob Van Arsdalen has been a great help so far. He knows everything that there is to know about Information Security. Every time I would have trouble with a project he would stop what he is doing to make sure I get the job done right. So far, this experience has been the highlight of my college career. I am very blessed to be able to have a yearlong internship for NASA.