IT Security Support for Spaceport Command and Control System

Jeffrey McLain

Kennedy Space Center

Major: Information Technology

KSC-FO Fall Session

November 27, 2013

Abstract

During the fall 2013 semester, I worked at the Kennedy Space Center as an IT Security Intern in support of the Spaceport Command and Control System under the guidance of the IT Security Lead Engineer. Some of my responsibilities included assisting with security plan documentation collection, system hardware and software inventory, and malicious code and malware scanning. Throughout the semester, I had the opportunity to work on a wide range of security related projects. However, there are three projects in particular that stand out. The first project I completed was updating a large interactive spreadsheet that details the SANS Institute's "Top 20 Critical Security Controls." My task was to add in all of the new commercial of the shelf (COTS) software listed on the SANS website that can be used to meet their Top 20 controls. In total, there are 153 unique security tools listed by SANS that meet one or more of their 20 controls. My second project was the creation of a database that will allow my mentor to keep track of the work done by the contractors that report to him in a more efficient manner by recording events as they occur throughout the quarter. Lastly, I expanded upon a security assessment of the Linux machines being used on center that I began last semester. To do this, I used a vulnerability and configuration tool that scans hosts remotely through the network and presents the user with an abundance of information detailing each machine's configuration. The experience I gained from working on each of these projects has been invaluable, and I look forward to returning in the spring semester to continue working with the IT Security team.

Position Description

During the fall 2013 semester, I worked at the Kennedy Space Center as an IT Security Intern in support of the Spaceport Command and Control System under the guidance of the IT Security Lead Engineer. My responsibilities included assisting with security plan documentation collection; system hardware and software inventory; malicious code and malware scanning; intrusion detection; security assessments; vulnerability assessments and reporting; patch reporting; risk assessments; analysis of ports, protocols, and services associated with vulnerabilities; verification and validation of security hardware location and assignment; and software license tracking verification and validation.

Projects

Throughout the semester, I had the opportunity to work on a wide range of security related projects. This section will explain in detail three of the largest and most important projects I completed during this time. Each of these projects provided me valuable exposure to, and experience within, the real world environment of IT Security.

SANS Top 20

My first major task was to update a large interactive spreadsheet that details the SANS Institute's "Top 20 Critical Security Controls." The Critical Security Controls effort focuses first on prioritizing security functions that are effective against the latest Advanced Targeted Threats, with a strong emphasis on security controls where products, processes, architectures and services are in use that have demonstrated real world effectiveness. Standardization and automation is another top priority, to gain operational efficiencies while also improving effectiveness.

For each of the 20 controls, the spreadsheet explains the control and its requirements, what tests to perform to make sure the requirements of the control are met, common attack vectors that would compromise a system that doesn't meet the requirements of the control, as well as a list of commercial off the shelf (COTS) software that could be used to meet the requirements of the control. Each of the controls is also mapped to the National Institute of Standards and Technology's (NIST) Special Publication 800-53 Revision 3. This publication spells out the security requirements for information systems that all federal agencies must meet. My task was to update all references to 800-53 Revision 3 to the recently released Revision 4, as well as updating and adding in all of the new COTS software listed on the SANS website. In total, there are 153 unique security tools listed by SANS that meet one or more of their 20 controls.

Performance Tracking Database

One of the other major projects I completed this semester was the creation of a database that will allow my mentor to keep track of the work done by the contractors that report to him in a more efficient manner. At the end of the quarter, my mentor must fill out a performance review for each contractor and how they performed based on a list of predefined criteria. To help him accomplish this, the database I created uses an input form with drop-down menus so that he can record events as they happen throughout the quarter. I also created another form that allows him to drill down into the data to reorganize it and display specific records, such as by employee or by task order. At the end of the quarter after all of the events have been entered, he can use a report I created that groups all of his comments by task order and criteria. There is also a separate query that will display the average score given to each event by task order and criteria. By using this database to record events as they occur throughout the quarter, it will allow him to be more efficient with his time, as well as provide a more accurate review of the work performed by the contractors throughout the entire quarter.

Linux Assessment

Lastly, I have expanded upon a security assessment of the Linux machines being used on center that I began last semester. To do this, I used a vulnerability and configuration tool that scans hosts remotely through the network and presents the user with an abundance of information detailing each machine's configuration. For the purposes of this project however, I focused specifically on analyzing open ports, patches and updates that have not been applied, vulnerable services that are currently running, password policy, local user accounts and groups, and NIST 800-53 policy violations for each individual machine. By gathering all of this information and presenting it to the appropriate parties, they can take the steps needed to close any gaps in each system's security posture. It may sound cliché, but with security you are truly only as strong as your weakest link. It only takes one unsecure system to cause a major security breach. Completing this project gave me hands-on experience with a tool I had never used before, and my mentor now turns to me when he needs any custom reports created with this tool.

Conclusion

I have really enjoyed my time here this semester at the Kennedy Space Center. I got to work with some incredible people that were always available to help me with any question or problem I had. I am grateful that I was actually given challenging and important work that will help KSC achieve its missions. The experience I gained has been invaluable, and I look forward to returning in the spring semester to continue working with the IT Security team.