Kim Harrison, CETPA CTO Mentor Candidate

CONTEXT:

To demonstrate my understanding of network security, I have created an artifact that describes the use of the Nessus tool to identify vulnerabilities and have applied this information to correct critical and high vulnerabilities and minimize medium vulnerabilities through working with the Systems Engineers. In addition, i have implemented practices to maintain a secure network on a quarterly schedule.

LEARNING OUTCOME:

This artifact addresses the following Learning Outcomes from the *Cyber Security Fundamentals* class.

> **SeF-05. Demonstrate a working knowledge of one or more tools used in network security.**
> **SeF-06. Demonstrate the ability to apply what they have learned from SANS Security Control network security tools to improve network security.**

REFLECTION:

The network vulnerabilities artifact demonstrates the use of Nessus tool to identify the existing external vulnerabilities within the Washington Unified network which provided context for a discussion with the technology team to resolve the critical and high vulnerabilities in order to create a more secure network environment. The artifact includes a description of the high risk vulnerabilities and descriptions of how these vulnerabilities were resolved following the meeting with the department's Systems Engineers and the results of a second, or post, scan that reveals no critical or high vulnerabilities in the external network. Next steps for maintaining a secure network are described and include a quarterly maintenance schedule for all servers within the district as well as the purchase and implementation of the Nessus tool to perform quarterly scans. The next step stemmed from a review of the vulnerabilities and the discussion of how to best manage network security in a timely fashion and encapsulates the collective thinking of myself and the Systems Engineers. The artifact demonstrates mastery of utilizing one or more outside tools to examine the external network and through working with the Systems Engineers, applying what is learned to resolve vulnerabilities and put into place a proactive plan to prevent future critical and high risk vulnerabilities to reside within the network, both externally and internally.

Upon learning about the Nessus network tool and seeing the 10 critical and high vulnerabilities identified in the scan, I was alarmed and concerned. Reviewing the scan more closely, I realized that many of the solutions called for installing a patch and then began to question as to why the patches are not routinely installed, what is needed to maintain the security of the network, and what services

are we providing through the different open ports that were scanned. I informed the Systems Engineers that I had performed a scan on the external network and met with them to review the findings. In the meeting, I tried to not place blame as to why the scans turned up critical and high vulnerabilities but questioned to understand and learn from the engineers. At first the engineers were somewhat defensive as they iterated that they had already installed patches on some of the servers as a result of a major email incident and that they do not have time to routinely run upgrades and patches to the servers. Both shared that they understood the importance of maintaining a secure environment but explained that it was impossible to guard against every vulnerability. As the meeting progressed and we examined each port and the corresponding data, I felt that the anxiety level of the engineers decrease as they realized that I was seeking to better understand the functions of the ports and not to place blame. At the conclusion of the meeting, my initial thoughts about the solutions were reaffirmed and I was assured that many of the patches had already been installed and that they would follow up on the servers that were unknown based upon the limited information from the scan. We met the following day and the engineers shared that they were able to identify all of the servers, disable those that were not in use, and believed that all of the critical areas had been patched. I ran the Nessus scan a second time and noticed that not all of the ports came back on the scan and that all of the critical and high areas were resolved. To be proactive in maintaining the security of the network, I offered to purchase the Nessus tool for both external and internal scanning and the engineers were tasked with developing a quarterly schedule to routinely check for patches and updates on all of the servers so as not to reach a critical or high vulnerability over an extended period of time. They will provide me with the schedule at the next department meeting.

My learning about network security was substantial as a result of the creation of this artifact. Not having a network background and inheriting a network that was designed prior to my arrival, I had concerns of how security and efficiency of the network. I learned that there are very easy to use tools that will provide a fairly indepth reporting of vulnerabilities within the network and that this report, when couched correctly, can create a productive conversation that leads to resolving network vulnerabilities and launches a more general conversation about practices for securing our network. From this knowledge, I applied my new learning to create a system that is more proactive in maintaining a secure environment. Because I do not have a foundation in network security, the learning that took place as a result of this artifact empowered me by providing the tools to form an understanding of my district's network environment. Additionally, implementing the protocol for continuous monitoring of systems on a quarterly basis on a rolling basis (not all reviews of the network will be completed on one day within the quarter but instead will be divided and reviewed across the quarter) can be utilized for a number of other systems and processes within the technology department. Updating inventory, collecting and dispersing of e-waste, check for software updates, and employee evaluations could all be completed quarterly using this model.

As a CTO, I am ultimately responsible for the security of the network and must rely upon the skills and knowledge of my technical staff that manage the network. By not having the skills and expertise to manage the network at the level needed to maintain security, I must have a general understanding of the work involved and be able to foster a relationship in which I can both direct and learn from my technical staff. This artifact not only increased my knowledge about the security of the district's

external network, but provided the development of a system for staying current on upgrades that includes ongoing dialogue around network security. My practice as a CTO has changed because I feel that I now have the knowledge to have conversations about network security in a way that is not accusatory or based upon my perception of the network.