Security Fundamentals Reflection

Cindy Patterson, CETPA CTO Mentor Candidate

Outcomes

SeF-06. Demonstrate a working knowledge of one or more tools used in network security.

SeF-08. Demonstrate the ability to apply what they've learned from network security tools to improve network security.

Context

The Santa Clara County Office of Education Technology Services Branch separates duties as do many other IT operations and businesses. There is a group that is primarily responsible for the customer facing activities and a second group that is responsible for infrastructure responsibilities. The group that is more customer-facing is Technology Programs and Instructional Support. Technology Programs and Instructional Support is comprised of 3 groups; Educational Technology, Web Development and Technology Resource Advisors. I manage the Technology Resource Advisors group which support Enterprise Level off-the-shelf software with the majority of our focus on the ERP system. I have worked in network operations at other entities in the past however it has not been my area of focus nor responsibility for the last 10 years.

SCCOE provides various networking services to districts in Santa Clara and San Benito counties. The operations of Santa Clara County Office of Education span a large geographical region for various different business units that range from a science camp in the mountains to Special Education in urban areas. This entire infrastructure is maintained by a few dedicated individuals who are very seasoned and astute.

Artifact

The artifact presented is a Nessus vulnerability scan of the SCCOE network; 1,637 pages. The report provides summaries in several different ways and detailed information about each item identified as vulnerability.

Reflection

During this exercise I became more aware of the efforts of our SCCOE ISC team to maintain security and learned about security tools. I discussed my assignment with our network manager and obtained permission to scan a portion of our network using Nessus and the corresponding IP addresses. I performed the scan on Friday evening to avoid any impact to the

operation. By performing the Nessus scan on the SCCOE network I have demonstrated a working knowledge of tool used in network security achieving the desired outcome SeF-06.

This exercise demonstrated to me how much network security has grown in size and complexity in the last 10 years and the need for a multiple layer approach. Throughout the report there were references to databases of known threats which were very interesting. I found myself drilling, and drilling down more. This was incredibly interesting but also incredibly time consuming. I became intrigued with what certifications were available for this specialty and reviewed the requirements for CISSP.

The information about the state of the World Wide Web that Aaron shared changed my point of view. I assumed that United States was the leader in technology use. He said there are an estimated 3 billion internet users. Other countries are growing faster than we are and have more population. Other new information was the internet of things and security. The 5 technology things that will change our world 3D printing, Robots, Driverless Cars, The All-IP World, Haptic Interfaces. This was a very exciting thought. Aaron also focused on privacy and the role of the CTO. The information about Electronic Information Privacy Acts was new to me and will be very helpful in my role as a CTO.

As a manager in the Technology Services Branch I will advocate for more resources for network security. This exercise has opened a dialogue about priorities and staffing. I am more aware of privacy issues, types of attacks, multi layered defense and available tools. Therefore I am better prepared to support an LEA and apply what I have learned to improve network security as a CTO.