During my training and preparation for my Security+ exam I took some online training from CompTIA which helped greatly and allowed me to do projects related to the concepts on the exam and gain practical experience. These projects include Performing vulnerability scans, Implementing a firewall, Using group policy, performing reconnaissance, implementing allow and deny lists, configuring system monitoring, and performing digital forensics.

The most impactful project I had during this training involved responding to a network incident using a variety of tools and techniques. Firstly, it involved analyzing network traffic from an already existing pcap file on Wireshark in order to find any external or malicious IP addresses. Next, I had to review the machine targeted by the malicious IP, discover any active connections, check for any unauthorized accounts, and finally check for anomalous processes. Next, I used windows event viewer to perform a log analysis on the windows security logs, then comparing logs to the pcap file for any matching malicious IP addresses. After comparing and validating a malicious incident occurred, my results showed a malicious program was running in the background, and an unauthorized administrator account was created. Next, I implemented mitigation by disabling/removing any malicious programs, and disabling any unauthorized user accounts. Finally, I verified all malicious activity was suspended, and that there were no malicious packets being transmitted in Wireshark.