Collegiate Cyber Defense Competition Review

By Shane Evans

 This year was IUS’s second year participating at the Collegiate Cyber Defense Competition, a contest designed to give college students hands-on experience in defending a computer network against hackers. It was my first year participating, but I feel like I did pretty well in handling both the expected and the unexpected challenges presented by the contest.

 The format of the event is like this: universities and colleges send teams (called blue teams) to defend virtual networks. The virtual networks are accessed using some proprietary software that I had never seen before this event, but they behaved like real machines. The virtual network is supposed to be run by some sort of business that needs to host a web server, mail server, ftp, etc., so blue teams can’t just unplug everything. In addition to securing the networks and maintaining uptime, we also had to field a number of requests from the hypothetical business running our network. These requests (called “injections”) were usually sensible, like implementing a strong password policy or adding two new users. Some injections were kind of silly in the context of the competition, like drafting a notice about employee usage of social networks or doing your boss’s kid’s homework. For one injection, two of our members were randomly called out to a fake meeting.

 The challenges came from the initial setup of the network. It wasn’t secure at all, so before we could do much of anything, we had to change passwords, delete rootkits, and update old software. The network was deliberately left vulnerable to basic attacks. After securing the network, the majority of the event was spent either wondering why things didn’t work quite right or dealing with injections. Injections were unexpectedly brutal and sometimes had very short deadlines so you could not easily look up how to do them. There were about thirty injections over eight hours and we did about half of them.

 There is no scoring after first and second place, so I can’t be positive how we did. We seem to have done pretty well in securing the network, though. Both preparing for the event and participating in the event were enormously instructive and I feel like securing a small computer network is now within my abilities. I’m eager to go back next year and do even better.