Cyber Security Day: Creating a Mock Cyber Competition Event to Increase Student Interest in Cyber Security

Thomas R. Imboden
timboden@siu.edu

Nancy L. Martin
nlmartin@siu.edu

Belle S. Woodward
bellew@siu.edu

Marcus E. Wood
Mearlwood48@siu.edu

Joshua Goodman
Joshuagoodman92@siu.edu

Southern Illinois University
Carbondale, IL 62901, USA

Abstract

Recent high profile security breaches at private and government organizations and reports predicting large deficits in the number of qualified information security personnel required in the near future illustrate the need for college students studying in this area. This paper describes the evolution of Cyber Security Day, an event focused on increasing student interest in studying cyber security in college and as a potential career field. Through the hosting of a mock cyber defense competition during an annual Cyber Security Day, the authors have demonstrated that such active learning events and activities successfully increase student interest in the cyber security career path.

Keywords: Information security, security education, cyber competitions

1. INTRODUCTION

Today cell phones, broadband connections, and the increasing reliance on digital systems in all areas of our lives have created more opportunities for cyber criminals. Countless examples of intrusions and high profile hacking incidents illustrate a glaring fact: the need for cyber security professionals remains unmet. The International Information Systems Security Certification Consortium predicts in their 2015 Global Information Security Workforce Study that there will be a shortage of 1.5 million information security professionals in the next five years (Frost & Sullivan, 2015). According to the Cisco 2014 Annual Security Report, globally there is a shortage of an estimated 1 million information security staff and managers (Cisco, 2014). There is a deficit of trained cyber security specialists within the workforce of the government and industries in the U.S. The lack of this workforce makes it difficult for government and the private sector to build technical cyber proficiency within the U.S. and across the globe. This shortage in qualified information security personnel is aggravated by the recent rise of sophisticated cyber attacks against organizations ranging from international corporations to state and federal governments. As educators, it is critical that we actively encourage students to consider information assurance and security as a potential career path in order to help meet the need for qualified security professionals.

Providing students with interesting and engaging events, opportunities, and experiences is one way educators can work to encourage student interest in information technology and security as a career path. This paper discusses the evolution of a Cyber Security Day event at a large, Midwestern university (http://isat.siu.edu/activities/cyber-days/) and the effect that incorporating a mock cyber defense competition into the event has had on increasing student interest in cyber security. Over four years, the annual event has quadrupled in participation, fostered collaborative learning partnerships with regional colleges, strengthened bonds with alumni, and most importantly has offered engaging and useful learning opportunities for student event volunteers and attendees. Through successful activities and events such as Cyber Security Day and the associated mock competition, interest in information security and awareness of the university's success in the field has increased, which the authors strongly believe will result in growth in enrollment in the information security program and in the workforce.

The authors, a group consisting of both information security-focused faculty and undergraduate students studying information assurance, describe the preparation and execution of Cyber Security Day including a mock cyber defense competition. The paper provides recommendations and guidance for others hoping to create a similar event, discussing methods for reaching potential participants and for developing the infrastructure necessary for a mock competition. Also presented is advice on creating regional partnerships with other institutions, maintaining strong ties with alumni, and most importantly, creating an exciting and engaging opportunity for active learning through the hosting of a mock cyber defense competition. Finally, participant feedback supporting the success in increasing interest in the information security program and career field will be shared.

2. BACKGROUND

The information security program at the authors' institution has a strong, 10+ year record of producing graduates who obtain employment in information assurance and security roles. Graduates work at organizations ranging from small, local businesses to global corporations to the federal government and defense department. These alumni perform a diverse set of duties including:

- vulnerability assessment and mitigation
- public key infrastructure administration
- secure network design
- penetration testing
- corporate application security verification
- DDoS mitigation and research
- security education
- disaster recovery and business continuity planning

In addition to traditional academic and classroom activities, students studying information assurance and security are actively encouraged by faculty and program administration to participate in co-curricular activities. These include becoming members in registered student organizations (RSOs) with a technology focus. One such organization engages student participants in planning and preparation for competing in cyber security exercises and competitions. This has led to the team earning several state championships and participation in regional cyber defense tournaments. Another RSO encourages learning outside the classroom by performing volunteer technical work for local nonprofit groups and by regularly hosting IT industry experts who discuss their careers and experience in the field. It has been shown that participation in such co-curricular activities positively influences student success (Elliot, 2009; Garcia, 2010; Montelongo, 2002). In planning for Cyber Security Day, the support and collaboration with the leadership of co-curricular RSOs is essential to success. The design and implementation of the mock competition held during Cyber Security Day was exclusively performed by these student volunteers, who spent countless hours preparing and learning new skills and technologies for the event. It is the opinion of the authors that this participation and the personal investment student volunteers contribute increases future alumni engagement and support for the program as well.

3. EVOLUTION OF CYBER SECURITY DAY

Understanding the critical need for properly trained security practitioners and the projected need for more in the foreseeable future, the authors firmly believe that events such as Cyber Security Day, which encourage involvement in security related activities and groups, is one important way to increase program enrollment, improve retention, and contribute to the training of qualified personnel the future workforce needs. Over four years, the event has evolved from relying primarily on experienced security experts speaking on related topics to hosting a successful mock cyber defense competition supporting over forty student competitors.

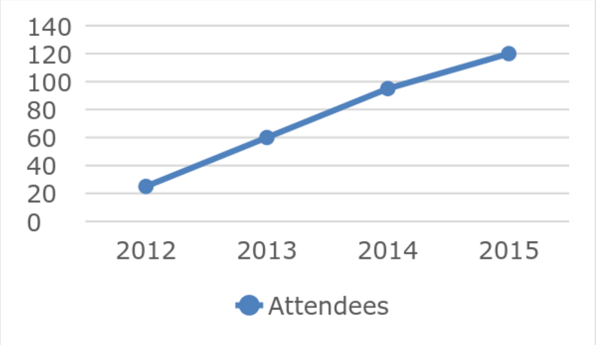


Figure 1: Attendee Growth

The first Cyber Security Day in 2012 included participants from the host university and a regional community college. This represented approximately 25 students and three faculty. Two speakers discussed the information security career field and participants were treated to a light breakfast, lunch, and were given a custom designed souvenir t-shirt.

Cyber Security Day in 2013 had significantly higher attendance and participation. The program's faculty set a goal to visit additional regional community colleges to encourage participation in the upcoming event. Approximately 60 participants attended the four-hour event.

The event in 2014 saw a dramatic increase in participation and featured the first attempt at a mock competition. The structure and organization of the mock competition is discussed at length in the next section, but the authors believe its introduction contributed significantly to the increase in attendance. Approximately 95 attendees from four community colleges and two high schools participated. Several institutions had enough students attending to field their own eight-person team for the mock competition.

The most recent Cyber Security Day, hosted in April of 2015, was the best attended event so far, drawing approximately 120 participants from eight regional colleges, three high schools, and from the local community. The event included six different security experts as speakers, five of which were university alumni and three were program alumni. Students from the program offered demonstrations of security and privacy related projects created during academic course work. A student panel of eight current and former cyber defense team competitors discussed their experiences preparing for and competing in recent collegiate cyber defense competitions. Speakers were selected based on their background or experience in information security, or a related field, and were asked to speak for approximately twenty minutes. Short five minute demonstrations of security tips or tools were performed by students in between speakers.

The highlight of the 2015 Cyber Security Day was a two-hour mock cyber defense competition. The authors believed the mock competition would provide attendees with an engaging and fun activity that would encourage interest in participating in future competitive cyber security activities and in studying cyber security. Additional details on the mock competition are provided in section 5.

4. ENCOURAGING PARTICIPATION

Over the previous four years, a lot has been learned about what does and does not work when reaching out to potential attendees and students. Each person who attends an event might be a future student and security professional. This section describes some methods the authors from the four-year institution (host school) have utilized to reach students and faculty who may be interested in participating in Cyber Security Day or similar events. It should be noted that the authors have concentrated these efforts on two year community colleges and local high schools.

Establish Relationships with Other Schools
Over the course of several years, the authors have identified, and now have established strong relationships with, faculty at community colleges within an approximately 150 mile driving distance from the host university. Faculty began by identifying key counterparts or program coordinators in the information security area and introducing themselves and the program at the host university. In general, the faculty at the two year colleges were very receptive to learning about transfer programs and other learning opportunities for their students. Faculty then visited security courses or student group meetings at the two year schools. This provides the host institution faculty a direct means of discussing relevant learning opportunities with students and faculty and providing them with a personal invitation to an upcoming event.

The authors maintain an updated email list of faculty from the regional schools for the purpose of exchanging relevant news and other information. For example, when information regarding instructor training opportunities or newly established educational and industry partnerships are created, this information is shared with the group of faculty. Engaging in useful and relevant dialog throughout the school year helps to maintain good communication between faculty and colleagues.

Share Learning Opportunities
Through the relationships with faculty colleagues, opportunities to share educational experiences between schools typically exist. For example, classes and student groups from the host university regularly provide remote colleges the opportunity to participate when speakers come to discuss interesting topics. Schools that might be too far to drive for an hour presentation are easily able to attend via webcast. The authors have found this to be reciprocated, having had students and faculty at the host school invited to attend events at the other schools.

Share Resources
Depending on the institution and state, some schools may have access to more technical resources than others. For example, the authors' university owns and maintains a NETLAB+ system for offering remote virtual labs. This system has been at times shared with other schools who have used the tool in their own classrooms.

Formalize the Partnership
Most recently, the host university has established an informal cooperative group from which events and activities can be driven. A web site which publicly acknowledges the partnership with the participating schools is being created and will be used as a venue for more publicly sharing learning opportunities with other institutions and the community. It also provides a venue for prospective students to find additional information when searching for educational opportunities.

Rely on Alumni
Program alumni can be great advocates and supporters of events such as Cyber Security Day. Maintaining communication with alumni and relying on their expertise for assistance with events and activities such as Cyber Security Day is critical. Alumni have invested significant time while a student in the program and many will continue well after they have graduated.

Contact Local Media
With the number of breaches and hacking incidents that have occurred recently, the media are aware of the importance of cyber security. By working with campus media and communications personnel, it is often possible to obtain publicity before the event in order to reach out and to invite participants. Several media outlets have even invited the authors for interviews on television and radio in order to help get the word out about the Cyber Security Day event.

Provide Food and Gifts at the Event
Students love pizza and free gifts. The authors have found inexpensive gifts like flash drives and gift cards to be great door prizes at the end of the day. Local restaurants and computer stores have traditionally been very generous with items to use as door prizes. While somewhat more expensive, t-shirts are perhaps the best giveaway. They provide a means of promoting the host school and event for years to come every time a participant wears them.

5. ACTIVE LEARNING THROUGH A MOCK CYBER DEFENSE COMPETITION

Security competitions such as the National Collegiate Cyber Defense Competition (CCDC), the US National Security Agency's Cyber Defense Exercise (CDX), and DEFCON Capture the Flag (CTF) have gained popularity in the last decade. The mock competition held at Cyber Security Day was designed using the CCDC as a model. Student volunteers experienced in cyber defense competitions provided help to mock competition participants, many of which had little to no experience with information security let alone cyber competitions.

The mock competition was designed by members of an RSO at the host institution and was inspired by and modeled after the CCDC events organized by the Center for Systems Security and Information Assurance (CSSIA). The host university has participated in CCDCs that CSSIA administers for many years and their success and professionalism provided an excellent framework for how the Cyber Security Day mock competition should be conducted.

The CCDC events and the mock competition are exclusively focused on cyber defense; no active "hacking" against other teams or attempts to "capture flags" are allowed by the teams competing. Two main types of groups actively participate in the competitions. The "blue teams" consist of the student participants that are tasked with defending the systems and networks within the competition. Each blue team consists of eight participants and the host school's infrastructure allowed for six separate blue teams. The "red team" consists of a group of current and former students and alumni who were participants in previous cyber defense contests. The red team's goal is to hack into the blue teams' networks and systems throughout the mock competition. The blue teams at this year's event were widely varied. Two schools had enough students to field their own eight person blue team and one high school did as well. Other blue teams consisted of smaller groups from colleges and high schools placed together to create teams with eight participants.

The premise for the mock competition, and many CCDC events, is that blue teams are the newly hired staff for a fictitious corporation. They are told that the previous information technology (IT) staff had been fired and that they are tasked with entering into an unknown environment and must attempt to take over managing the fictitious corporation's systems and network. The blue teams are each assigned their own "pod" which consists of a number of computer and network systems for which they are responsible. These systems, typically virtual machines, are both Microsoft Windows and Linux, server and client, and are in varying states of function and levels of security when the competition begins. An example of one blue team pod is available in Appendix A. Each blue team is assigned their own pod and all are identical with the exception of IP addresses. Each pod connects to the "ISP", a single virtual network that allows teams access to the Internet and provides connectivity to the red team as well. This network connectivity allows the red team to conduct reconnaissance and attacks against the blue teams. The entirety of all the blue team pods, the red team pod, and associated infrastructure and networks make up the Cyber Stadium used for the competition.

At the start of the mock competition, teams must evaluate and determine the state of their assigned systems, conduct system hardening activities, and perform other tasks required by an IT team. In addition to these administrative and security tasks, teams are asked to complete tasks that were designed to simulate those an IT team might be required to perform in a workplace. These tasks are called "business injects". Business injects are designed to evaluate a variety of the blue teams' skills. Business injects varied in requirements. Examples of injects potentially assigned in the competition include:

- Create an inventory of all systems and services
- Develop an acceptable use policy for the organization
- Add a new user for a particular system or service
- Create cryptographic hashes of specific files on systems
- Install a centralized logging server

The blue teams must do their best to defend their simulated enterprise network from a wide range of attacks performed by the red team while they work on injects, update and harden their systems, and remove any malicious software that may have been installed before they took over as the IT team for the fictitious corporation.

A "white team", composed of student and faculty volunteers, takes on the role of the blue teams' corporate management, such as the CIO of the company. It is the white team's responsibility to distribute the business injects, review completed business injects, and provide feedback and assistance to the blue teams when necessary. In the formal CCDC events, there are additional teams dedicated to judging, technical support, and hospitality that were not deemed necessary for a mock competition.

Three components make up the final score for each blue team during an official collegiate cyber defense competition event. These are service availability (uptime), business inject completion, and red team success at infiltrating blue team systems and networks. As blue teams assume the role of an enterprise IT team, they are responsible for maintaining availability for specific services running on certain systems in their pod. For example, they may have to ensure that a web server located on a system on their DMZ is available for access. A scoring engine system checks for service availability as seen from "outside" the blue team's network, simulating how a public facing service would be accessed from a remote, internet client.

A web-based application was created for the distribution and submission of injects and for measuring blue team system uptime. Once again, the application was modeled after one created by CSSIA, however, was built from scratch by student volunteers. Using Ruby on Rails, the web application provides a user interface for blue teams as well as the white team. The white team issues the business injects to all blue teams, which then view each inject through the web application. Once completed, blue teams submit their completed business injects, usually by typing required information into text documents or by including screenshots into the blue team's interface (Appendix B). The white team can then access the submissions and use the system to mark whether the business injects are completed satisfactorily.

The Cyber Stadium was built on the host university's VMware cluster with an NDG NETLAB+ system providing blue team pod access. All systems employed in the Cyber Stadium are virtual machines. The NDG NETLAB+ system allows participants access to the virtual environment through a web browser. Blue teams connect to the host university's NETLAB+ system, are presented with the topology diagram for their individual pod (Appendix A), and then click a particular system's icon in order to gain access to that virtual machine. Student volunteers built the Cyber Stadium that is used in the mock competition. This includes creating each virtual machine and appropriately preparing and configuring it as desired for the competition. The individual blue team pods each consisted of eight virtual machines and three virtual switched networks, a routing infrastructure, core firewall, and a variety of virtual switched segments which were necessary to provide connectivity between the blue team pods and the required competition infrastructure and provided pods internet access. Preventative measures were taken to ensure that no malicious traffic would leave the Cyber Stadium by employing firewall and filtering technology where the competition virtual networks connect to the physical, campus area network.

A scoring engine to evaluate the blue team's performance was integrated into the web-based inject assignment and submission system. It is designed to measure availability of specific services for each blue team. The scoring engine evaluates availability by regularly attempting to connect to each blue teams' systems and services that are required to be available throughout the competition. The scoring engine allowed each blue team the ability to view a dashboard displaying the status of their required available services (Appendix B). Teams can quickly determine whether a service is available (green indicator) or unavailable (red indicator). The blue team interface allowed each team member to view the status of each of their team's scored services. An administration interface allowed for the white team to view the status of every blue team's services.

6. ANALYSIS OF MOCK COMPETITION PARTICIPANT FEEDBACK

Since the main objective of hosting the Cyber Security Day event, and specifically the mock competition, is to increase student participant interest in studying information security, it was necessary to measure whether this goal was achieved. At the conclusion of Cyber Security Day, a short survey was given to all student mock competition participants who volunteered to complete it (n=39). Due to university recommendations regarding the participation of minors in survey projects, high school students were not asked to participate in the survey. The survey asked questions about student participants' perceptions of the mock competition such as whether it was well organized, if it was a good learning experience, if the mock competition increased interest in the cybersecurity profession, if the mock competition increased interest in studying cyber security, and if they would recommend participating in the mock competition to other students.

Based on the survey responses, the mock competition provided a positive experience that increased interest in the field and provided a greater understanding of the study of cybersecurity. Eighty-one percent of respondents indicated they had a good learning experience (Appendix C), 72% felt that the competition increased their interest in the cyber security profession (Appendix D), and 72% reported increased interest in studying cyber security (Appendix E). Eighty-five percent reported that they would recommend participating in the mock competition to other students (Appendix F). These survey results will serve as a benchmark for future competitions.

7. CONCLUSIONS

Over the course of several years, the Cyber Security Day event has evolved and transformed. The goal, to increase participant interest in studying cyber security and considering the area as a career field, has remained consistent. The methods and means the host university and authors have used to increase student participant interest in cyber security have changed. With initial data indicating that the mock competition strongly increases student interest in cyber security, the authors plan to further expand the mock competition in future Cyber Security Day events. Several ideas for improving the mock competition have been discussed:

- Providing training videos and remote access to the Cyber Stadium pods before the event to allow participants to better understand how to use the Cyber Stadium before the mock competition.
- Increase the length of the mock competition from two hours to four hours.
- Provide blue teams with fun post-competition awards such as "Best Inject Completion" and "Highest Uptime" as a way to recognize teams while still remaining a "mock" competition.
- Creating smaller pods with fewer virtual machines to allow for smaller blue teams, further increasing the amount of interaction required among teams.
- Decreasing the number of Linux virtual machines in blue team pods. Student participants seemed unfamiliar with Linux, especially the high school participants.

In conclusion, the success of Cyber Security Day and the mock competition in increasing interest in the career field and in studying cyber security has been validated on a small scale. As future events are held, and the improvements mentioned previously are implemented, these efforts will help fulfill the nation's need for qualified cyber security professionals. The authors wholeheartedly encourage faculty and students at other institutions to develop similar activities in order to further student interest in cyber security.

8. REFERENCES

Cisco (2014). Cisco 2014 Annual Security Report. Retrieved July 9, 2015 from http://goo.gl/zAvh0S.

Elliott, J. (2009). The Relationship of Involvement in Co-Curricular Programs on Community College Student Success and Development. (Unpublished doctoral dissertation). Lincoln, Nebraska.

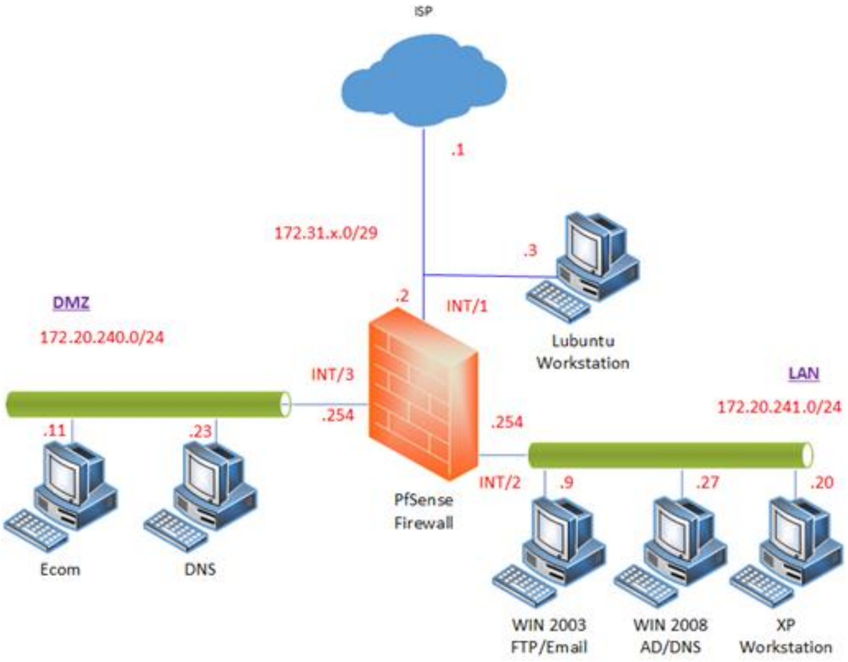
Frost, & Sullivan (2015). The 2015 (ISC)^2 Global Information Security Workforce Study. Retrieved July 9, 2015 from https://goo.gl/InyEGc .

Garcia, A. (2010). First Generation College Students: How Co-Curricular Involvement Can Assist with Success. *The Vermont Connection 31, 46-52.*

Montelongo, R. (2002). Student Participation in College Student Organizations: A Review of Literature. *Journal of the Indiana University Students Personnel Association*, 50-63.

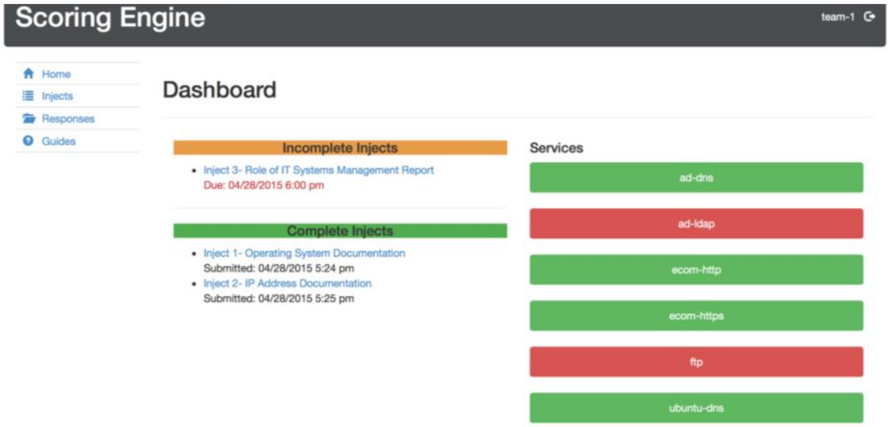
Appendix A

Example of Blue Team Pod Topology



Appendix B

Blue Team Scoring Engine View



Dashboard

Incomplete Injects

- Inject 3- Role of IT Systems Management Report
  Due: 04/28/2015 6:00 pm

Complete Injects

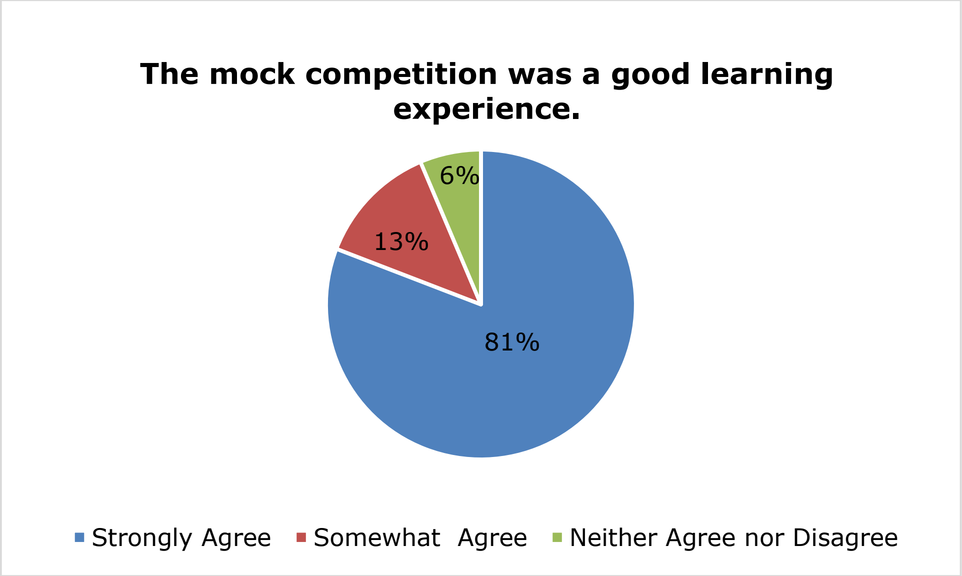
- Inject 1- Operating System Documentation
  Submitted: 04/28/2015 5:24 pm
- Inject 2- IP Address Documentation
  Submitted: 04/28/2015 5:25 pm

Services

🟩 ad-dns
🟥 ad-ldap
🟩 ecom-http
🟩 ecom-https
🟥 ftp
🟩 ubuntu-dns

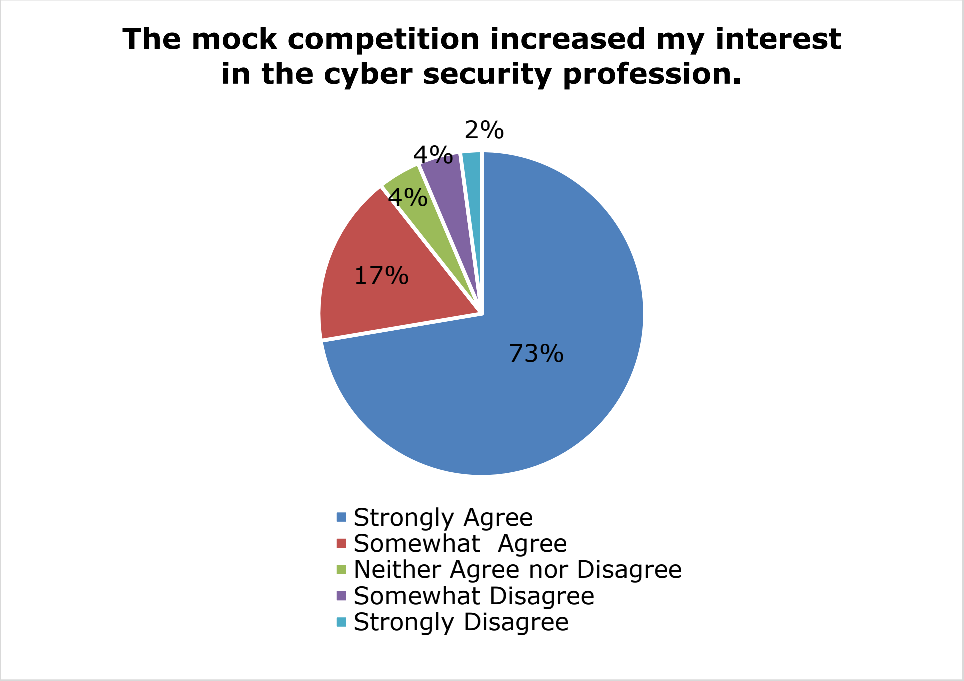
Appendix C

Good Learning Experience



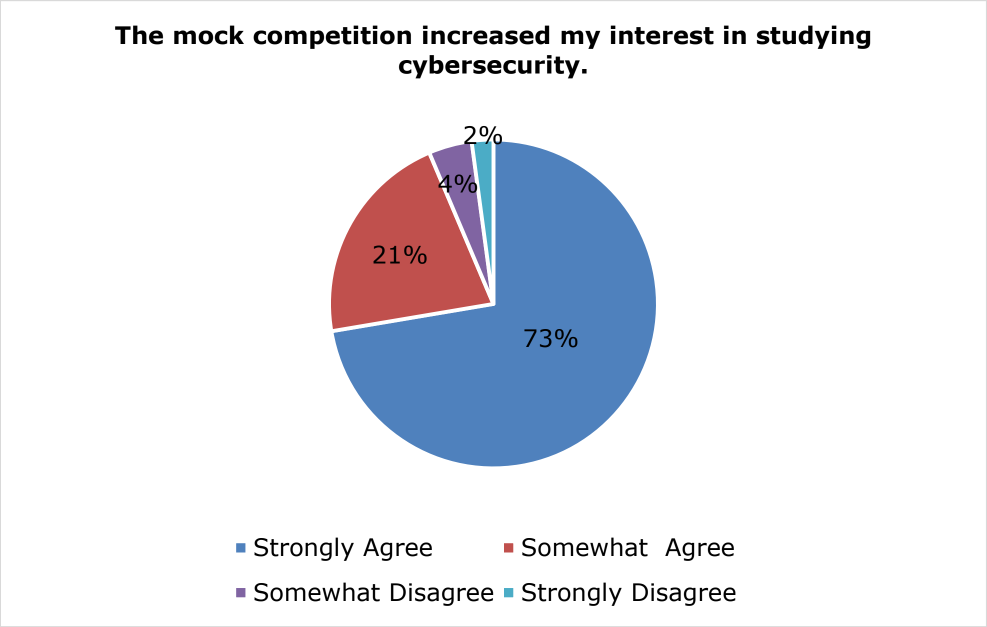
Appendix D

Increased Interest in Cyber Security Profession



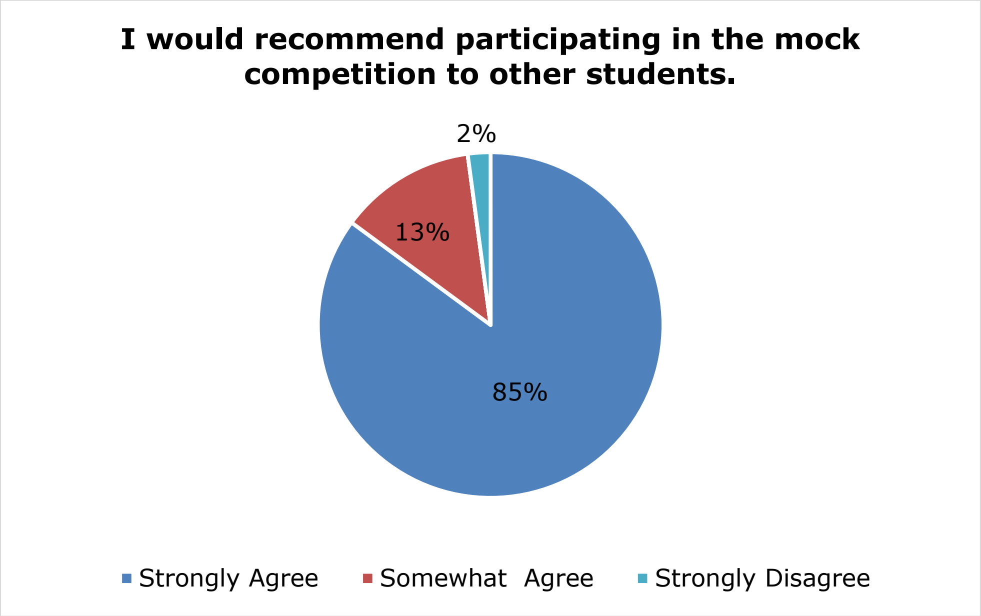
Appendix E

Increased Interest in Cyber Security Profession



Appendix F

Would Recommend Participating to Other Students


I would recommend participating in the mock competition to other students.
■ Strongly Agree
■ Somewhat Agree
■ Strongly Disagree