Creating a Deep Learning Environment in a Virtual Lab for Cybersecurity

Randall Joyce
Murray State University, rjoyce@murraystate.edu

Brandon Dixon
Murray State University, bdixon2@murraystate.edu

Abdul Yarali
Murray State University, ayarali@murraystate.edu

Author Biography

Dr. Randall Joyce is an instructor at Murray State University in the TSM program,where he lectures students in the areas of cybersecurity, virtualization, and wireless. Randall holds an M.S in Health Informatics from Northern Kentucky University, M.S. in Telecommunications Systems Management from Murray State University, and B.S. in Telecommunications Systems Management from Murray State University. Randall has also recently completed his Ed.D in P-20 and Community Leadership with STEM Specialization from Murray State University.

Mr. Brandon Dixon is an instructor at Murray State University, holding a Bachelor of Science in Computer Science and Mathematics, as well as a Masters Degree in Telecommunication Systems Management. He has worked in the technology field for 14 years, spending four years at the Commonwealth Office of Technology in Kentucky. He then moved to Murray to work in the Information Systems program at Murray State University, where he spent nine years working with networking and security. Brandon has been involved in the development of our wireless and networking laboratories in addition to leading student recruitment efforts by directing networking security activities at Murray State University.

Professor Abdul R. Yarali received his BS, MS, and Ph.D. in Electrical Engineering from the University of Florida, George Washington University, and Virginia Polytechnic Institute and State University respectively. Dr. Yarali has worked chiefly in the field of wireless mobile communications technology as a technical advisor, engineering director, and now as a professor at Murray State University (MSU), Murray, KY. Dr. Yarali is the author of books in wireless systems, IoT, Privacy, Security and Trust in the cloud, and Big Data. He has been the editor of the journals, magazines, and books in wireless communications areas.

2019 Pedagogicon Proceedings

Creating a Deep Learning Environment in a Virtual Lab for Cybersecurity

Randall Joyce, Brandon Dixon, and Abdul Yarali
Murray State University

In today's world, there is an increasing need for cybersecurity professionals because of the increase of Internet-connected devices, digital assets, and information systems infrastructure. Growth of automation and digitization, enterprise safety risks, the illusion of privacy and consumer data breaching, data storage, and management in the world of massive internet device connectivity that is expected in the near future collectively bring new security concerns. In order for students to gain the required skill sets to enter the workforce, they need hands-on experience to build essential employability qualities, confidence, knowledge, and experience. Murray State University's Telecommunications Systems Management program uses a lab environment that has been developed using Netlab software to create a secure environment isolated from the campus network, allowing students to experience the execution of these attacks and exploits.

Introduction

The demand for higher education to develop trained cybersecurity professionals is growing with the increased need for cybersecurity professionals in the information technology industry. The United States Bureau of Labor Statistics predicted that by 2022, there would be a shortage of cybersecurity professionals close to 1.8 million (Frost & Sullivan. 2017). With those statistics reporting such short supply, it is apparent that students enrolling and graduating from cybersecurity programs should now be a priority. Often, students learn and retain cybersecurity skills through a series of hands-on activities and experiences that help prepare them for careers after higher education. Developing an environment where both on campus students and remote students can get hands-on experience with different cybersecurity applications and tools is critical for the students to have a profound learning experience that instills confidence in them with their skill sets (Ciampa, 2012). In the Murray State University Telecommunications Systems Management program, such an in-depth learning experience is accomplished for both on-campus and remote students by utilizing a program called Netlab to create an online cybersecurity lab environment (Dinita, Wilson, Winckles, Cirstea, & Jones, 2012). The Netlab environment provides students with virtual machines that exist in isolation from the central campus network infrastructure, providing them a safe and secure environment to test the different security exploits and applications (Imboden, Martin, Woodward,

Wood, & Goodman, 2015). Often these exercises are led with lab instructions in order to teach students the fundamentals as they advance through the program, requiring them to build upon what they have learned previously.

Program context

Students can experience deep learning through challenging cybersecurity exercises hosted in a virtual lab environment, requiring them to apply research skills and scaffolding experience to create real-world scenarios mirror experiences in industry. Teaching students how to research and solve cybersecurity challenges that occur in an enterprise environment on a daily basis is critical in preparing them for their career. This process allows students to learn the process they would go through for solving the issue and to teach them what resources are available to them to use to solve these issues as they arise through this methodology.

Strategy Overview

The methodology that is used in the virtual lab is based off the challenge-based learning model. In the challenge-based learning framework, the problems that students are given are often tied to an idea of global importance like war or sustainability of water (Johnson, Smith, Smythe, & Varon, 2009). We have adapted this model to the ideas of cybersecurity concepts and challenges, such as how to configure a mid-sized enterprise network using the best security practices or asking what kind of encryption would be used in low bandwidth networks to secure two sites. The adapted model can be seen in the following Figure 1, Deeper Learning by Challenging. Students are given these challenges and can use any resources they have available to them, along with the virtual labs, to come up with a solution for the problem (Cirstea, 2003). In the adapted model, students review the security concepts in class during a lecture and are provided the opportunity to ask and email any questions they have about the topic. Then they are given a challenge that emphasizes the concept and are provided lab materials such as guides, instructional manuals, and guided questions to help them develop and steer their solution. Students will then submit their solution to be reviewed and critiqued to gain feedback on what they did well (or not so well) to highlight how they can grow and develop from the experience. The use of a challenge-based learning framework helps guide the design of the lab material that is deployed in the virtual labs, where students can get basic cybersecurity fundamentals that they can build upon and develop into a stronger education in cybersecurity.

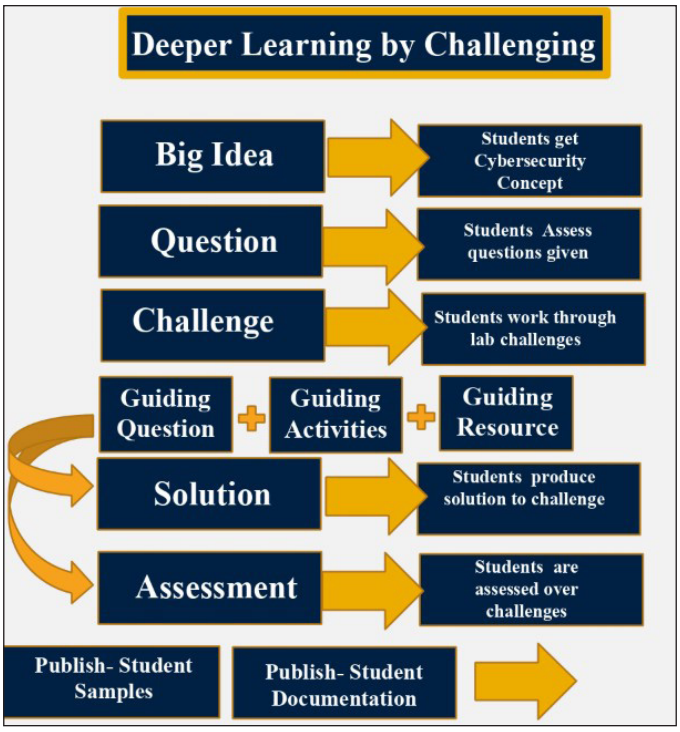

Figure 1. Deeper Learning by Challenging

Analysis

The use of a challenge-based learning framework to create a deep learning environment in a virtual lab has been an excellent experience for the students. Utilizing an online lab for both on-campus and remote students gives them the flexibility to log in from any location and work on enterprise-level equipment (Smith & Bluck, 2010). Giving students a chance to work on enterprise-level equipment is critical in developing familiarity and confidence in their skills and knowledge (Martin & Woodward, 2013), as well as preparing them for the field. This design does meet with one major challenge, which is the fact that it requires a large budget and consistent availability of resources. However, this lab format prepares students for working in the technology field where the technology is not in the same building or across the country. Working on the virtual lab infrastructure also gives students a sense of freedom where they can take their time and work through the labs at their own pace and they have time to research for the solution to solve the issue, as opposed to time constraints present in traditional class-time labs. Learning to research is one of the most valuable skills that students going into cybersecurity can have since in industry, as they will have to research to resolve and troubleshoot issues in the field. By having the virtual labs in Netlab configured in such a way that it requires students to do research and go through the challenge-based learning framework, enforcement of this methodology ensures that they will carry on with this type of research in their career fields. With this challenging learning model, the students are often pulled into the lab experience and feel ownership of the problem, increasing the

desire to resolve them successfully. The process that the challenge-based learning model leads students through causes them develop a robust research background that will be critical in their future education and career.

Discussion

Overall, utilizing the Netlab environment leads students through a challenge-based learning model in their lab work. It is critical in providing hands-on experience in cybersecurity to the students to prepare them for their career, and having this deep learning experience of researching to resolve issues remotely is a great advantage to student development (Martin & Woodward, 2013). In their careers, they may have the same flexibility that the Netlab offers in their job where they work remotely. Facilitating the experience of working on a device that they don't have physical access to, and facing the caveats that come with it, allows them to understand that the decisions they make while working on it are critical (Smith & Bluck, 2010). The Netlab environment provides a safe space for them to learn all the different cybersecurity tools that there are without repercussions if something does not go as planned (Imboden et al., 2015). Using virtual labs in the Netlab program is an excellent way of providing students with hands-on experience with cybersecurity tools that will help develop their knowledge and prepare them for the field.

Conclusion

In conclusion, the cybersecurity field not only needs more professionals, it needs professionals with relevant experience. It is critical for undergraduate programs to recruit, retain, and graduate students in the cybersecurity field who possess this experience. Undergraduate students will be in high demand, and once they complete their degree in cybersecurity, they will be filling the entry level cybersecurity jobs. Applying the challenge-based learning framework is a way to create a deep learning environment that challenges the students to use and develop skills they will need in their education and career. With the shortage of cybersecurity professionals currently and the forecasted shortage looming on the horizon, it is critical to get students involved in cybersecurity and to provide a secure and flexible lab environment in which they can grow and learn, which will help foster their interest in cybersecurity.

References

Ciampa, Mark. (2012). *Security+ guide to network security fundamentals* (4th ed.). Boston, MA: Cengage Learning.

Cirstea, M. N. (2003). Problem Based Learning in Microelectronics. *International Journal of Engineering Education*, 19(5), 738-741.

Dinita, R. I., Wilson, G., Winckles, A., Cirstea, M., & Jones, A. (2012). A cloud-based virtual computing laboratory for teaching computer networks. *13th International Conference on Optimization of Electrical and Electronic Equipment (OPTIM)* (pp. 1314-1318). Talk presented

at 13th International Conference on Optimization of Electrical and Electronic Equipment in Brasov, Romania.

Frost, A., & Sullivan Executive Briefing. (2017). Global Information Security Workforce Study. Retrieved from https://iamcybersafe.org/wpcontent/uploads/2017/06/Europe-GISWS-Report.pdf

Johnson, L. F., Smith, R. S., Smythe, J. T., & Varon, R. K. (2009). *Challenge-based learning: An approach for our time* (pp. 1-38). Austin, TX: The New Media Consortium.

Imboden, T. R., Martin, N. L., Woodward, B. S., Wood, M. E., & Goodman, J. (2015). Cyber security day: Creating a mock cyber competition event to increase student interest in cyber security. *Proceedings of the EDSIG Conference* (p. n3481). Talk presented at EDSIG Conference in Wilmington, N.C.

Martin, N. L., & Woodward, B. (2013). Building a cybersecurity workforce with remote labs. *Information Systems Education Journal*, *11*(2), 57.

Smith, A., & Bluck, C. (2010). Multiuser collaborative practical learning using packet tracer. In *2010 Sixth International Conference on Networking and Services* (pp. 356-362). Presented in Cancun, Mexico.