Problem-based Learning for Cybersecurity Education

Mandar Shivapurkar
School of Computer Science and Engineering
Sacred Heart University
Fairfield, CT, USA
shivapurkarm@mail.sacredheart.edu

Sajal Bhatia
School of Computer Science and Engineering
Sacred Heart University
Fairfield, CT, USA
bhatias@sacredheart.edu

Irfan Ahmed
Department of Compter Science, College of Engineering Virginia Commonwealth University
Richmond, VA, USA
iahmed3@vcu.edu

***Abstract*—Traditional lecture-based approach with laboratory-based exercises is commonly used to teach cybersecurity. It is useful to provide hands-on experience to students. However, it fails to provide students an opportunity to completely explore the multi-faceted and ill-defined problems prevalent in the real-world cybersecurity scenarios. Problem-based learning is a student-centered pedagogy in which students are presented with complex, open-ended, real-world problems to promote learning of concepts and principles, contrary to the traditional lecture-style presentations. Over the years, the model has been adopted to teach concepts in other disciplines including economics, business administration, architecture, law, engineering and social work, however, there has been little work done in the field of cybersecurity. This paper illustrates the use of problem-based learning for cybersecurity education along-with an open cyber range architecture for preliminary implementation. This student-focused and active learning pedagogy has proven to not only provide students with an opportunity to learn relevant concepts, tools and techniques applicable to the given problem but also improve focus, interest, motivation, and foster lifelong learning skills, essential to survive in ever-changing cybersecurity field.**

Keywords—problem-based learning, cybersecurity education, problem-solving skills, critical thinking

I. INTRODUCTION

Cybersecurity instructors combine traditional lectures with hands-on lab exercises to improve the student learning outcomes. Based on our experience, an overwhelming majority of the available cybersecurity hands-on exercises fall well short of what is needed. They typically follow a cookbook approach and consists of a series of steps presented to students to follow; they are rarely designed to build problem solving skills and deep understanding of cybersecurity concepts [1]–[6].

In our view, problem-based learning (PBL) holds considerable promise in helping to improve learning outcomes in cybersecurity education. Problem-based learning is a student-centered pedagogy in which students are presented with complex, open-ended, real-world problems to promote learning of concepts and principles, contrary to the traditional lecture-style presentations [7]. In addition to covering domain-specific concepts, problem-based learning approach also fosters critical thinking, develops problem-solving, writing, communication and collaboration skills, enhances motivation to learn and retention of information, and promotes self-directed and lifelong learning [8].

Problem-based learning was pioneered by Barrows and originally used for medical education [9], [10]. Over the years, the model has been adopted to teach concepts in other disciplines including economics and business administration [11], architecture, law, engineering and social work [11], [12]. Unfortunately, problem-based learning has not been explored systematically for cybersecurity education.

In problem-based learning, the teacher acts as a facilitator and a mentor rather than the source of solution and presents the students with a problem instead of lectures and assignments. As the students are not handed with any content, the learning becomes more active and encourages students to explore and work with the specific contents identified as important by the teacher to find a solution to the problem.

In this paper, we illustrate a problem-based learning method (by Maastricht [13]) in the context of cybersecurity education by mapping the working model of the method to two cybersecurity scenarios. The authors believe that such an interactive and student-focused learning environment will not only help students to understand the complex nature of attack and defense mechanisms but will also give them a holistic view of multi-faceted real-world scenarios, in-turn promoting critical thinking and problem-solving skills.

The remainder of the paper is organized as follows. Section 2 discusses the related work followed by the section 3 to describe problem-based learning pedagogy and its implementation details on two cybersecurity scenarios. Section 5 provides summary and directions for future work in this area.

II. RELATED WORK

This section discusses the current state of the problem-based learning.

A. Existing Use of Problem-based Learning

According to Wood [14], utilization of resources and tutor facilitation are the issues which makes it difficult for schools or colleges to adapt PBL. It requires the educators to

979-8-6425-4896-7/20/$26.00 ©2020 CISSE

take an active role in facilitation where some of them find this more frustrating. On the other hand, it is resource-intensive because it requires more physical space and more accessible computer resources.

In 1969, the medical school at McMaster University has introduced an approach to teach medicine using problem-based learning[1]. The course focuses on providing the groups with realistic case thus expecting the students to study, research and come up with findings in the following week. By using this method in their postdoctoral program, it helps the students to identify their strengths and weaknesses in that content area. University of Missouri School of Medicine did a research for 10 years and indicated that PBL has a positive effect on the students competency as physicians after graduation [15].

PBL is introduced across wide areas of studies. Problem-based learning was introduced in the field of Engineering and Humanities lectures in the University Tun Hussein Onn Malaysia in the collaboration with the Aalborg University Denmark [16]. This project involved 30 academic staff who were selected from six faculties and two academic centers, 220 undergraduates were selected using purposive sampling. It was revealed that students not only were benefited in the content area but also in generic skills such as leadership, analytical thinking, conflict management and decision making. Students said that despite of greater amount of work, it was compensated with the knowledge and skills they obtained. They further added that it would have been depriving if the teaching had been conducted using the conventional way.

B. *Effectiveness of Problem-based Learning*

The effectiveness of the problem-based learning is dominantly evaluated in the field of medicine [13]. For instance, it is explored in nursing education to prepare nursing professionals for a growing range of patient care services. Shin and Kim reported that problem-based learning has positive effects on student satisfaction with training, clinical education, and skills development [13], [17]. Furthermore, Oja reported a positive impact on nursing students critical thinking [18]. More recently, Loyens et al. [19] compare the effectiveness of three pedagogical methods: problem-based learning, traditional lecture-based, and self-study. They randomly assign students to one of the three group types, and use conceptual tests immediately after the lesson and post-test after one week. The evaluation results conclude that the students in problem-based learning group have a higher likelihood of conceptual change. Strobel and Barneveld [20] perform meta-analysis on problem-based learning by quantitatively synthesizing research results of previously separate but related studies, involving various statistical methods to retrieve, select, and combine effect sizes and results of the studies. They conclude that problem-based learning is an effective approach to "train competent and skilled practitioners and to promote long-term retention of knowledge and skills acquired during the learning experience".

III. Problem-based Learning for Cybersecurity

A. *Motivation*

The authors possess more than 10 years of combined cybersecurity teaching experience in five universities spanned across three countries. They have taught a broad spectrum of cybersecurity courses including network security, ethical hacking and vulnerability management. Generally, these course have been offered in more-or-less a traditional setting which combines lecture-based pedagogy with some laboratory-based hands-on assignments. Some of the common feedback comments from the students on the course content and instruction methodology are: more theory and less hands-on component, very specific lab assignments, and insufficient real-world scenarios. Some of the students have also mentioned the lack of problem-solving, critical thinking, communication and collaboration skills.

Problem-based learning is promising to address the challenges in cybersecurity education. Unfortunately, the pedagogy has not been explored systematically in cybersecurity. We only found one study on problem-based learning in the context of cybersecurity. The study is performed in the United Kingdom. However, the teaching material, implementation, and student experiences are not publicly available[2]. The preliminary study used case studies and scenarios for the problems, and measure students' summative performance, student engagement and confidence, and reported promising results. Thus, in this paper, we demonstrate how a problem-based learning method can be utilized for cybersecurity education.

B. *Problem-based Learning Pedagogy*

We use Maastricht's method on problem-based learning, which is divided into a seven-jump process [9]:

1. Clarify terms and objects: Identify and clarify unfamiliar terms presented in the scenario.
2. Defining the problem: Define the problem or problems to be discussed.
3. Brainstorming: Aspects on basis of prior knowledge are collected.
4. Structuring and hypothesis: Review steps 2 and 3 and arrange explanations into tentative solutions. During the fourth step, which forms the core of the analysis, the problem is explained on different ways.
5. Learning objectives: Formulating learning objectives; group reaches consensus on the learning objectives; tutor ensures learning objectives are focused, achievable, comprehensive, and appropriate.
6. Independent Study: Self-independent learning; during this phase students can go home and study. This phase is supposed to provide answers to the questions evoked in the problem-analysis phase and offer students possibility to acquire a more profound knowledge of theories at the root of the problem.

[1] https://mdprogram.mcmaster.ca/mcmaster-md-program/overview/pbl—problem-based-learning

[2] https://www.heacademy.ac.uk/system/files/downloads/alastair_irons-problem_based_learning_in_cybersecurity.pdf

7. Synthesis: Group shares results of private study. The tutor checks learning and may assess the group. So, the final step is synthesizing and testing the newly acquired information.

Figure 1 presents the working model of a problem-based learning approach. There are various advantages of problem-based learning. PBL is student-focused, which allows for active learning, better understanding with integration of experience and knowledge, and retention of knowledge. It also helps to develop life skills that are applicable to many domains. It further enhances skills like communication and teamwork, critical thinking and questioning, problem solving and self-reliant learning.

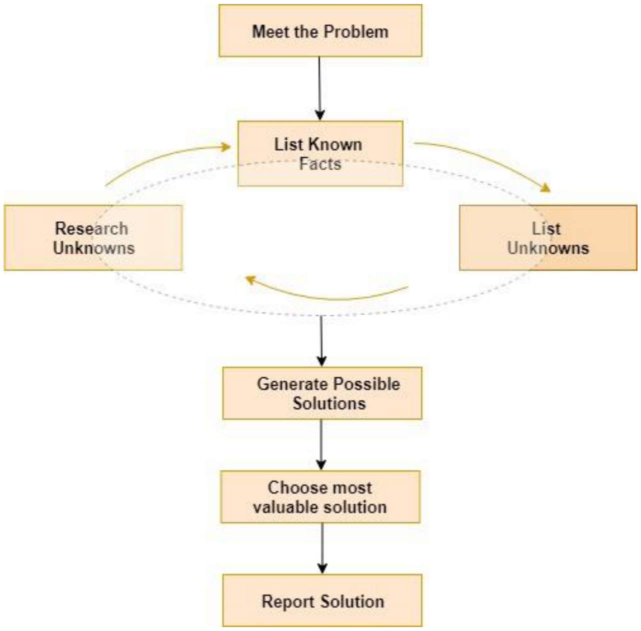

Fig. 1. Problem-based Learning Working Model

IV. Implementing Problem-based Learning in Cybersecurity

We demonstrate how Maastricht's method of problem-based learning can be applied on two different cybersecurity topics for illustration.

A. Cybersecurity Problem 1

To begin we will start with the top layer of OSI model (Figure 2), by introducing an email phishing example at the beginner level. Phishing is the most common way to gain sensitive information. Company staff like front desk operator, IT employee, managers and directors receive emails on daily basis. Many of these emails purporting to be from reputable companies to induce individuals to reveal personal information. In a traditional teaching approach, the instructor would present the concept and workings of a phishing email and the associated data loss with an example. Students rarely get an opportunity to create and launch phishing attacks and explore countermeasures if they receive such mails.

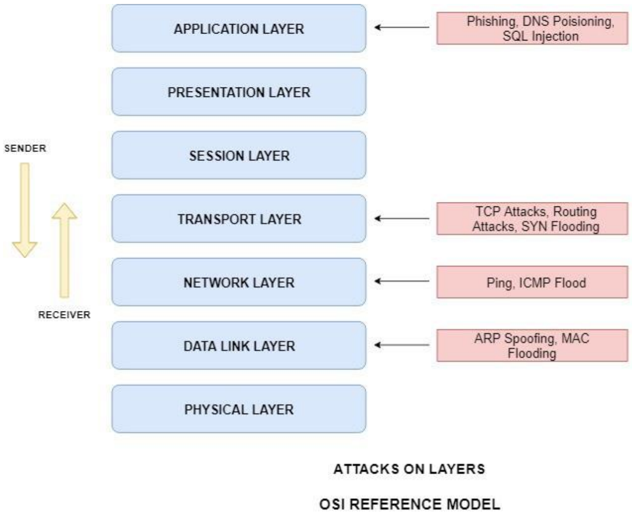

Fig. 2. Attacks on Layers of OSI Model

On the contrary the problem-based learning approach gives students complete knowledge over phishing with the help of the seven-jump process and an ill-faced example.

Problem Description: Suppose all front desk operators in a company receive an email from reputable ecommerce website. This email further asks the users to click on the link to activate a $150 coupon code. Following this event, the organization saw a rapid change in their database. How can an attacker create such emails?

Step 1: Clarifying terms and objects gives the students a basic idea on the concept they are going to study which is phishing for this example. Groups can be created in this process with students of different background to help increase the quality of the research.

Step 2: Defining the problem, as the problem is ill-structured the above example is discussed by the instructor without revealing enough information.

Step 3: Brainstorming, by learning from the above ill-structured example students must bring their prior phishing knowledge on the table. This step helps to identify how much Knowledge they have on the current topic.

Step 4: Structuring and hypothesis, students must think about the problem in different ways like, what can be the factor behind this rapid change in the database? What different tools the attacker could have used to create this phishing mail and gain access over the database? Is there a possible malware/backdoor present? With the help of different questions, students can create hypothesis for the problem.

Step 5: Learning objectives can put on the table by the groups, instructor needs to make sure that the students are not mislead and continue the correct path.

Step 6: Independent study, students can use objectives from the previous step to find solutions for the problem. This step involves students to work individually. Due to the ill-structure, students needs to find different tools to attack the victim machines while they will now have various steps to secure the victim machine.

Step 7: Synthesis, this step individual work will be mapped together in the group and discussed the class. The complete self-learning process is accomplished in this step.

B. Cybersecurity Problem 2

Based on the importance of vulnerability management in the field of cybersecurity, we have created another example which targets the working knowledge of different Linux tools, firewall management and TCP/IP ports [21]. In a typical vulnerability management or related course, students are given a brief introduction on ports numbers, firewalls, scanning tools and techniques, and they are taught how to close certain open ports to avoid possible attacks. Learning firewall configuration only in theory is not enough to prepare them for the real-world scenarios. Misconfigured firewall has often led to many breaches in the past. It is imperative that the students are taught different mechanisms of firewalls such as OPEN, FILTERED and CLOSED and what they mean.

Problem-based learning helps students to think in a critical manner. They do not keep themselves dependent on a single factor to protect a machine but try to research and mitigate all possible vectors for the attack as illustrated in the example below (Figure 3).

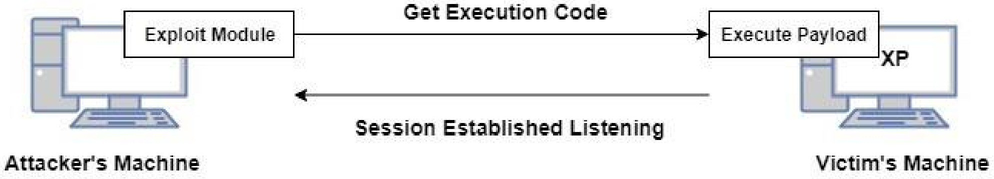

Fig. 3. Attack on SMB Port

Problem Description: Mr. Mike is a company secretary and he is working on companys confidential data on his Windows desktop. He saved his work in a folder name Secret Information and kept the system running. When he returned to his office on the next day, he was surprised to see that the file was missing. The investigating team claimed that the problem was in the SMB port of the system. Using the attackers machine, perform the above scenario on a Windows system. If successful, use various methods to protect the system and try the same attack again to ensure that the system is safe.

Step 1: Clarifying terms and objects, working in groups students must research on different terms like the port numbers, firewalls and its uses.

Step 2: Defining the problem, as the problem is ill-structured the above example is discussed by the instructor without revealing enough information.

Step 3: Brainstorming, as the port is specifically given to be SMB, students can share their knowledge on the SMB port and its usage with each other.

Step 4: Structuring and hypothesis, in the above example the operating system is mentioned as windows while a specific port has been mentioned, this makes students think on different attack vectors on a single port with different flavors of windows operating system. With the help of a structure they must come up with different hypothesis in this step.

Step 5: Learning objectives, ideas can be described by the students as what they have found out and their next strategy. Instructor needs to verify if they are on track and not mislead.

Step 6: Independent study. They must work individually and try to find solutions to the problem using a practical approach. With the help of different tools, they can try to attack various flavors of Windows operating systems on its SMB port, while they need to find a solution to protect against such attacks like properly configuring the firewall, implementing a network based firewall apart from host based, blacklisting or white-listing of the IP addresses, etc.

Step 7: Synthesis, individual work will be mapped together in the group and discussed in the class. Other groups can obtain information from this and understand the missing points.

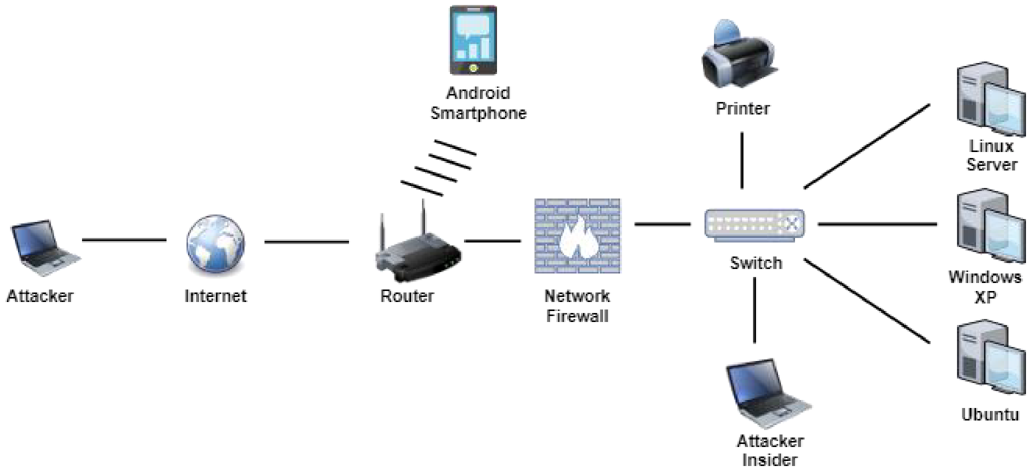

Fig. 4. Open Cyber Range Architecture

V. Cyber Range for Problem-based Learning

This section will describe the open cyber range architecture and its combination with problem-based learning pedagogy.

A. Open Cyber Range

A cyber range is a virtual environment that is used for cybersecurity training and development. It provides tools that help strengthen the stability, security and performance of cyber infrastructures and IT systems used by different organizations. There are several software's which are available to run cyber challenges. Most of these are proprietary and are very expensive. It is very difficult for the high schools and community colleges to purchase and maintain these software's.

To mitigate the budget problem and help students learn cybersecurity practically, we are building an open cyber range architecture. This architecture will contain off-the-shelf softwares which will result in cost-effectiveness. Open cyber range will incorporate pre-configured virtual machines. The architecture will help students learn configuring IDS/IPS devices, protecting devices like android smartphones, tablets, different flavors of Windows operating system and complex Linux environments.

Open cyber range requires less hardware infrastructure as it will be implemented in a single host machine. Minimizing the cost and time of building the complete virtual environment, it will be an ideal scenario for the colleges and working environments.

B. Red Team Vs Blue Team

Once the problem is solved by all the groups, entire class can be divided in two teams; red team and the blue team.

This concept is generally seen in the capture the flag events where the red team is the attacker team and the blue team is the defender team. Examples may contain practice on securing the database against SQL injection by using various techniques like stored procedure, using a problem and with the use of 7 step PBL process and open cyber range students can compete with each other. This method will help them gain confidence which can help them in the real world.

VI. Conclusion and Future Work

Cybersecurity education has traditionally been taught in a lecture-based setting with laboratory-based exercises which has been proved useful to provide students with hands-on experience. This approach, however, has failed to provide students the much-needed opportunity to comprehensively explore the multi-faceted and often ill-defined cybersecurity problems in real-world. Problem-based learning is a student-centric and active learning pedagogy which presents complex, open-ended and real-world problems to promote learning of concepts and principles. We have illustrated the use of problem-based learning for cybersecurity education by mapping its working model to two cybersecurity scenarios.

References

[1] I. Ahmed and V. Roussev, “Peer instruction teaching methodology for cybersecurity education,” *IEEE Security & Privacy*, vol. 16, no. 4, pp. 88–91, 2018.

[2] P. Deshpande and I. Ahmed, “Topological scoring of concept maps for cybersecurity education,” in *Proceedings of the 50th ACM Technical Symposium on Computer Science Education*. ACM, 2019, pp. 731–737.

[3] P. Deshpande, C. B. Lee, and I. Ahmed, “Evaluation of peer instruction for cybersecurity education,” in *Proceedings of the 50th ACM Technical Symposium on Computer Science Education*. ACM, 2019, pp. 720–725.

[4] M. Bhatt, I. Ahmed, and Z. Lin, “Using virtual machine introspection for operating systems security education,” in *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*. ACM, 2018, pp. 396–401.

[5] W. Johnson, I. Ahmed, V. Roussev, and C. B. Lee, “Peer instruction for digital forensics,” in 2017 *{USENIX} Workshop on Advances in Security Education* ({ASE} 17), 2017.

[6] W. E. Johnson, A. Luzader, I. Ahmed, V. Roussev, G. G. Richard III, and B. Lee, “Development of peer instruction questions for

cybersecurity education," in *2016 USENIX Workshop on Advances in Security Education (ASE 16)*, 2016.

[7] J. F. Barell, *Problem-based learning: An inquiry approach*. Corwin Press, 2006.

[8] B. J. Duch, S. E. Groh, and D. E. Allen, *The power of problem-based learning: a practical" how to" for teaching undergraduate courses in any discipline*. Stylus Publishing, LLC., 2001.

[9] H. S. Barrows, *How to design a problem-based curriculum for the preclinical years*. Springer Publishing Company New York, 1985, vol. 8.

[10] H. Barrows, "A taxonomy of problem-based learning methods," Medical Education, vol. 20, no. 6, pp. 481–486, 1986.

[11] W. Gijselaers, W. H. Gijselaers, D. T. Tempelaar, P. K. Keizer, J. M. Blommaert, E. M. Bernard, and H. Kasper, *Educational Innovation in Economics and Business Administration: The Case of Problem-Based Learning*. Springer Science & Business Media, 1995, vol. 1.

[12] D. Boud and G. Feletti, *The challenge of problem-based learning*. Routledge, 2013.

[13] E. H. Yew and K. Goh, "Problem-based learning: an overview of its process and impact on learning," *Health Professions Education*, vol. 2, no. 2, pp. 75–79, 2016.

[14] D. F. Wood, "Problem based learning," *Bmj*, vol. 326, no. 7384, pp. 328–330, 2003.

[15] M. Medicine. (2018) Students take active role in education with pbl. [Online; accessed 1-Jan-2020]. [Online]. Available: https://medicine.missouri.edu/news/students-take-active-role-education-pbl

[16] O. Hussain, B. Mohd, E. Ahmad, A. Selamat, and A. Sulaiman, "Problem-based learning across diverse engineering disciplines at universiti tun hussein onn malaysia," *International Journal of Learner Diversity*, vol. 1, pp. 113–126, 12 2009.

[17] I.-S. Shin and J.-H. Kim, "The effect of problem-based learning in nurs ing education: a meta-analysis," *Advances in Health Sciences Education*, vol. 18, no. 5, pp. 1103–1120, 2013.

[18] K. J. Oja, "Using problem-based learning in the clinical setting to improve nursing students critical thinking: an evidence review," *Journal of Nursing Education*, vol. 50, no. 3, pp. 145–151, 2011.

[19] S. M. Loyens, S. H. Jones, J. Mikkers, and T. van Gog, "Problem-based learning as a facilitator of conceptual change," *Learning and Instruction*, vol. 38, pp. 34–42, 2015.

[20] J. Strobel and A. Van Barneveld, "When is pbl more effective? a metasynthesis of meta-analyses comparing pbl to conventional classrooms," *Interdisciplinary Journal of Problem-based Learning*, vol. 3, no. 1, p. 4, 2009.

[21] S. Bhatia, S. Behal, and I. Ahmed, *Distributed Denial of Service Attacks and Defense Mechanisms: Current Landscape and Future Directions*. Cham: Springer International Publishing, 2018, pp. 55–97