Scenario Based Exercises in IA Courses

Nanette S. Poulios, *Walsh College*, and Dipesh Pradhan, *Walsh College*

Abstract – To address criticism of higher education pedagogy, scenario-based learning (SBL) is presented. Principles and learning methodologies from experiential learning theory are reviewed.The authors present practical methodology for a sample scenario incorporating scenario based learning.

Index terms – Information Assurance, scenario based learning, digital forensics

I. Introduction

College courses often use a didactic, lecture based delivery method. The basis for this type of delivery is often a textbook, lecture notes, and textbook problems or questions [1]. This didactic approach to teaching has been criticized by industry [2]. Corporations are increasingly demanding more from MBA students [3]. Few business schools include learning by doing. Students know theory but not how to solve problems in the real world. Many employers are finding that graduates are too narrowly focused on learning theory rather than problem solving [4]. Using a didactic approach, students may learn to solve problems using pre-defined sets of rules, but have difficulty extending this learning to other situations. The lecture approach is often ineffective when teaching students how to solve complex problems [1].

In the past, computer forensic education has often been taught by law enforcement rather than academic institutions. These have typically been five day intensive training courses. Currently, academic institutions are offering courses in digital or computer forensics within their information assurance degrees [4]. Too often, academic courses focus on knowledge, abstraction, and theory [4] while training courses focus on skills, application and practice. Certainly, both types of education are necessary to prepare students for a career in information assurance.

Today's student has grown up in an interactive environment [3]. These students expect a more interactive classroom experience than a didactic approach to classroom leaning. Students often express concern in programs where they expect hands-on-learning and instead are presented with lectures focusing on core knowledge [5]. Instructors are concerned about student retention when students become disillusioned early in a program. Scenario based learning (SBL) offers a solution to this on-going problem.

II. Learning Theory Background

Various learning styles and teaching methods exist in the education field. Several of these are of interest when using scenarios to teach real world problem solving. DA Kolb and A Kolb [7] express that learning is experiential. They refine the experiential learning theory (ELT) to include principles for the entire educational environment. The SBL model follows these principles [1].

The principles of ELT are:

- Learning is a process. Higher education should focus on engaging students in a process.
- All learning is relearning based on a student's beliefs and ideas.
- Learning resolves conflicts. Disagreement and differences drive the learning process through reflection, action, feeling and thinking.
- Learning is holistic and integrates cognition, thinking, feeling, perceiving and behaving.
- Learning is synergetic between a person and the environment. A student must apply existing concepts to new experiences.
- Learning creates knowledge unlike the transmission model where knowledge is transmitted to the learner [6].

Learners progress through this learning cycle experiencing, reflecting, thinking and acting. Thus learning occurs as a student advances through the cycle of concrete experience, reflective observation, abstract conceptualization, and active experimentation [2].

SBL uses a context where the problem is presented in a controlled sequence [3]. The student has to make choices to reach an outcome. This follows the ELT by providing students with an opportunity to experience, reflect, perceive, and behave or act. The student's actions affect the outcome of the scenario. The choice a student makes alters subsequent events or leads to new events. In these scenarios, learners may make a wrong choice; however, learning still occurs. The learner will learn from his mistakes rather than be penalized for wrong choices.

Nanette Poulios is the Director of the Information Assurance Center and an Associate Professor at Walsh College. Dipesh Pradhan is a recent Graduate of the MSIA program at Walsh College.

ISBN 1-933510-96-X/$15.00

SBL is based on the following premises:

- Reality is the best learning experience
- Learning should be fun
- Learning should allow for mistakes
- Real learning occurs when a student is immersed in a situation, provided feedback and allowed to adjust his responses [3].

SBL integrates concepts into the learning experience. Students must gather data to solve the scenario based problem. For example, Mariappan, Shih, and Schrader [3], devise a scenario based an engineering course. This scenario is based on the Hyatt Skywalk tragedy from 1981. A skywalk collapsed in Kansas City killing 114 people and injuring 200. Students were asked to investigate this accident. Their tasks are to discover the building code and check if the Skywalk met the code, analyze drawings, estimate load on the skywalk, and draw diagrams of original and modified designs. Students learn how vibrations and load affect lives. This scenario is much more effective than working on typical textbook problems.

III. Practice Methodology

SBL is a student centered approach to learning. Students are engaged in the active learning process. In order to be successful, students must develop research and problem solving skills. Instructors must be facilitators [5]. Several types of scenarios are possible. The first type is problem based learning which describes a scenario or problem with a predetermined outcome. This requires students to acquire and assimilate knowledge to solve a specific problem. Opposite this is project based learning where the outcome is open ended. Project learning focuses on the product [5].

SBL encourages students to draw on experience, knowledge and skills that have been presented in previous class sessions. Scenarios should be new applications of this knowledge. These situations should also be realistic and open-ended. Social aspects should also be incorporated into the tasks for solving the problem. Group projects allow students to develop team and management skills while reducing the management load on instructors and students [5].

Thomsen, Renaud, Savory, et al [5] recommend a five step process for adapting scenarios into the classroom. In order for students to succeed, the instructor must include checkpoints throughout the project. The first checkpoint is planning which includes problem definition, research, innovation, design concept, role assignment, and resource requirements. Checkpoint 2 two is the design stage. This is the refinement of the design conception into an actual solution with specifications. Checkpoint three is also a refinement stage. During this stage, the students build and test the subsections of the design and solve any identified problems. Validation is also included in this stage. The student must test and debug the solution. The final checkpoint is the actual reporting of the solution. This might include a group or individual presentation, posters, technical documentation or review of another group's project solution. Students also should submit a 1 to 2 page reflective summary of their learning and experience.

These checkpoints are recommended for a week long project. Students receive the project on a Monday. Checkpoints 1 and 2 occur early in the process, usually one or two days after the scenario is presented. This might be a short discussion with the instructor. On Thursday, the third checkpoint is assessed. These checkpoints ensure the groups are making progress [5]. This process could easily be adapted to a class that meets once a week as well. For example, in a 4 hour class, the scenario would be presented at the beginning of the class session. During the first hour, progress for checkpoints one and two could be assessed. Checkpoint 3 would be assessed at the end of the class. The project would be due at the next class session the following week.

Following these checkpoint and practice methodologies assures that student learning is occurring, errors are corrected early, and groups are progressing satisfactorily.

In order for the learning cycle to be complete, student work must be assessed, and the feedback cycle must be complete.

IV. Student Perceptions

Classroom studies show students have a positive attitude towards SBL [1, 3, 5]. Evaluations from an engineering course at Cal-Poly [1] indicate that increased learner interest in the subject and improved knowledge retention. In an experimental MBA marketing course [3], students rated the lecture approach very low and the simulation high. Students also rated how well each methodology taught specific skills such as problem solving, tea development, communication, problem solving strategic planning and risk taking. The simulation based scenario rated higher than lecture based learning in all areas but written communications. A telecommunications course [4] also had positive student feedback for an SBL project. Students reported that theories were easier to learn using an SBL project. In another trial engineering project [5], student excitement was high. Student feedback was extremely positive and engagement was high.

V. SAMPLE WORKSHOP

The following scenario was developed by a capstone student from Walsh College as his final capstone project. The scenario exercises were created with the guidance of his capstone instructor and an industry expert.

Often, computer users make common mistakes. Mistakes may happen due to one's negligence or because they are unaware of the vulnerability. Some common mistakes may include creating weak passwords, storing sensitive information on their local computer, leaving computers unpatched, ignoring company policies and standards, and running unnecessary services. They may not realize the risks that they expose for their organization's data, but intruders are always looking for such vulnerabilities to exploit. This project is closely designed with such common mistakes in mind. The project is developed in the form of a scenario based workshop. The workshop will provide security awareness to attendees and the requirement to consider security as an integral piece of the configuration. Since this is a scenario based workshop, students will receive actual hands on experience. In this information age, following information security best practices is not optional, but a must. This workshop is an example of problem based learning.

The workshop is based on a scenario using a computer to run business applications which becomes mysteriously infected; and someone is stealing sensitive information from that computer. Furthermore, the computer is not following information security best practices and has security vulnerabilities. Attendees will be presented with the company's security policy and standards.

The task objective is to audit the computer and determine the status of the infected computer. Within a limited time period, attendees will be asked to identify the vulnerabilities, discover the security holes, perform a forensic analysis, and correct the problem. Students will then document their findings in an Incident Report and Forensic Analysis form.

A. Overview

The purpose of this workshop is to provide an investigative activity that represents network and computer infestation and determine how effective the student feels the workshop is in attaining an awareness of security issues and formulating a goal oriented attitude that leads to identifying methods to prevent it. This is a problem solving task. The student is expected to use administrative skills in this workshop.

A production machine has been breached and the information taken contains PII (Personally Identifiable Information) data. In addition, the computer contains security vulnerabilities. Students need to i) investigate, ii) repair and iii) document the issue.

1. Assumptions

Students are expected to know how to read and analyze firewall logs and to have a working knowledge of common ports and basic Windows XP Professional administration skills.

2. Guidance

A Service Level Technology Use and Management Policy and Technology Standard documents for the production computer are provided to present (a subset of) operational configurations the computer is required to follow.

Students were given the following rules and directions for completing the exercise:

- Students are required to understand and check if the computer is in compliance with the company's security standard and policy.
- The effort of the audit process should be sufficient to lead them to identify the non-compliance issues, vulnerabilities, and the policy violations.
- Student teams are allowed to inquire of each other, to access the Internet and to use the various tools as described below in Tools section.
- Students are required to fix issues to resolve the problems.

3. Understanding

In a real forensic investigation, due process would require retaining the original machine state and imaging the computer to obtain a working forensic image. Due to the lack of time, short cuts are necessary to complete the investigation within the time allocated. Students were not required to image the computer. Instead they are required to correct vulnerabilities and log their actions.

4. Tools

The production machines contain TCPView and FPort tools that show the detailed listings of all TCP and UDP endpoints on the system, including the local and remote addresses and state of TCP connections. CobraSoft, a personal firewall log reader is also being provided.

Students were given the following instructions:

- TCPView can be run by clicking the TCPView icon present in Desktop.

- To run FPort, open the dos prompt by clicking on Start > Run and type 'cmd' (without apostrophe). When the dos prompt opens up, follow the following syntax:
  C:\> cd fport (you can type cd\ to go the root)
  C:\fport>fport

- CobraSoft – Personal Firewall LogReader, can be run by clicking PFWLogReader icon present in Desktop. Click on 'Open' and select the log file that you want to read.

B. Set-up Instructions

This workshop requires a VMware image (image to be provided upon request) of two computers. The first computer is a production machine which contains PII. The second machine is a rogue host. Both machines must be on the same network.

The following software and hardware components are required:

1. Software

- Filezilla Server
- Ftpconnect.bat file
- SalesData.exe Application
- Windows Firewall
- Microsoft .NET Framework 4
- TCPView
- FPort
- CobraSoft - Personal Firewall Log Reader

2. Hardware

- At least one production host (with Windows XP running windows firewall)
- At least one rogue computer.

3. Steps

Schedule SalesData Application in Production Host

- Create two different folders: "C:\Program Files\APS\Sales\Data" and " C:\Program Files\APS\Sales\EXE" .
- Insert the SalesData.exe in "C:\Program Files\APS\Sales\EXE" folder.
- In order to run SalesData.exe, the host requires .net framework (If it is not installed, it can be installed from **http://msdn.microsoft.com/en-us/netframework/aa569263).**
- To create a scheduled task to run salesData.exe in every minute, go to Start > Control Panel > Scheduled.
- Click on Add Scheduled Task and a pop up window appears. Click on Next to continue.
- Select "Command Prompt" application to run and click on next.
- Type "SalesData" as the name of the task and select "Daily" under perform this task menu.
- Select "Every Day" under perform this task menu. Select start time and start date and click on next to continue.
- Enter the password of the user. The username should be automatically populated. Click on Next to continue.
- Check on "Open advanced properties for the task when I click Finish" and click on Finish.
- Click on browse menu and navigate to the folder to find salesdata.exe. The path should be C:\Program Files\APS\Sales\EXE.
- Now, click on Schedule tab and click on "Advanced.." button.
- Check on Repeat task. Select "1" in every minute. Select "24" hours in duration and click on "Ok".
- Click on "OK" to close the window.
- Verify that the schedule is running and creating a salesdata.txt file in "C:\Program Files\APS\Sales\Data folder".

4. Install Filezilla Server

- Install Filezilla, the server Edition in production host (make sure it is server edition, not the client edition). The software is Open Source and can be downloaded from http://filezilla-project.org/download.php?type=server
- Create a user by going to Edit > Users. You can also create a user by clicking on  user icon at the menu bar.
- After creating the user, specify the specific location as "C:\Program Files\APS\Sales\Data" for the user by going to [Shared Folders] which can be see under Page section on the left hand side
- Close the Filezilla server by clicking on  icon. This shall close the Filezilla Server, but the application will run in background.
- Open the windows firewall by going to Start > Control Panel > Windows Firewall. Turn "off" the firewall by clicking "Off" if it is turned on.

5. Install ftpconnect.bat in Rogue Host

- Create a new folder in Rogue machine such as C:\Program Files\APS\SalesData\FTPConnect.

- Create another folder in Rogue machine such as C:\Program files\APS\SalesData\FTPConnect\FromProduction1.

Note: based on number of production machine, the number of folders can be increased as FromProduction1, FromProduction2.

- Insert the ftpconnect.bat inside that folder.
- Right click on ftpconnect.bat file and click on "Edit".
- Based on requirements, change the values of ftpconnect.bat file.
- Following is the content of the file,

  @ftp -i -s:"%~f0"&GOTO:EOF

  open 192.168.1.101 – enter the IP address of Production machine

  dipeshp – enter the username of the machine
  123123 – enter the password of the machine

  lcd C:\Program Files\APS\SalesData\FTPConnect\FromProduction1– enter the directory path in which you want to save the file

  mget salesdata.txt – enter the name of the file that you would like to get from production machine.

  disconnect

  bye

Note: Based on number of production machine, the new information can be appended to the same batch file or you can create new batch file with similar information.

- Now, you can schedule to run the batch file using Task Scheduler. The process is described in step 3. .

6. Windows Firewall

- Make sure that the windows firewall is turned off by going to Control Panel > Windows Firewall.
- Delete any old existing firewall logs to avoid any confusion.

7. IP configuration

- It is recommended to have the IP address of production machine as static IP Address.
- If you have the VMware image of production machine, you only need to change the IP address in ftpconnect.bat file of the rogue machine as described in step 5.

8. Internet Explorer Settings in Production Host

- Make sure the Internet Explorer version is 6.0
- Go to Internet Properties by right clicking on Internet Explorer icon
- Under general tab, point the homepage to the file 'google.html' that has been provided.

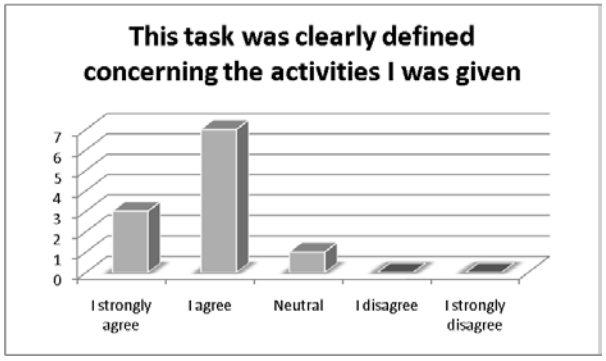
ISBN 1-933510-96-X/$15.00

9. Third Party Software

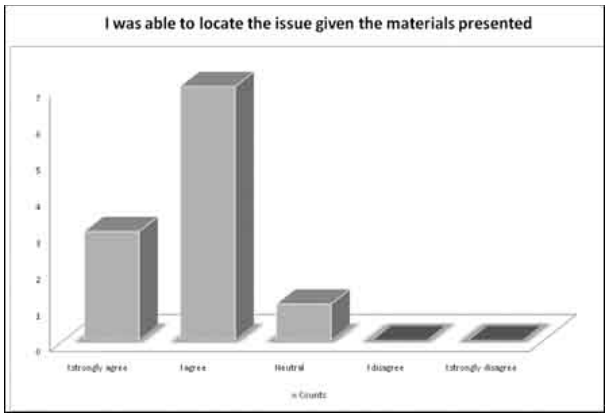
- **CobraSoft- Personal Firewall Log Reader** – this software can be downloaded from: http://www.cobrasoftonline.com/downloads/PFWLogReader.msi . Please make sure that there is a shortcut link in Desktop
- **FPort** – this software can be downloaded from. http://www.scanwith.com/download/Fport.htm Please make sure that you install this software under C:\Fport directory
- **TCPView** – this software can be installed from http://download.sysinternals.com/Files/TCPView.zip. Please make sure that there is a shortcut link in Deskop

C. Feedback Form Report

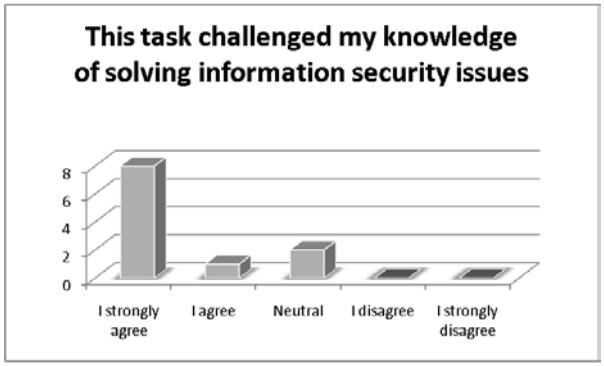
The Workshop was held at two locations. The first location was another Center of Academic Excellence (CAE), University of Detroit Mercy. The purpose of the first Workshop was to pilot the workshop and correct any errors in the lab set-up or instructions. The actual Workshop was held on Nov 17th at Walsh College, TroyCampus. Sixteen people registered for the workshop and fifteen students attended the workshop. Overall, students found the workshop educational and helpful. At the end of the workshop, students provided feedback on evaluation forms. Eleven students handed the feedback form and the data gathered can be found below:



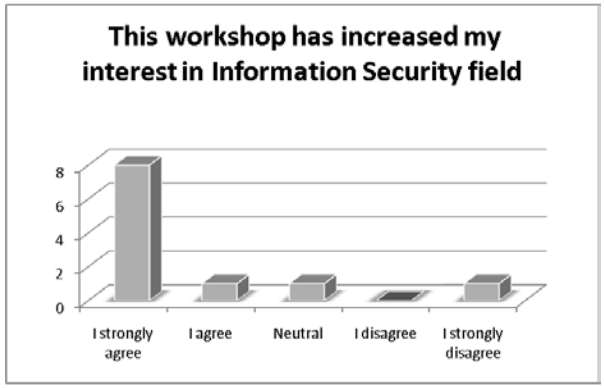
Question 1 Feedback



Question 2 Feedback



Question 3 Feedback



Question 4 Feedback

VI. Conclusion

Clearly this scenario based workshop follows the learning theory of allowing students to learn by experience. In this exercise, students learn that allowing vulnerabilities to exist may result in exposing PII data. Students are able to discover and mitigate these vulnerabilities as well as compare the configuration against published policies and standards. Student feedback was very positive with students reporting that they actually learned more from

this voluntary exercise than from written course assignments.

Full lab set-up guides, images, report forms, and students instructions will be made available to all attendees.

VII. References

[1] Mariappan, J., Shih, A., Schrader, P.G. (2004). Use of scenario-based learning approach in teaching statistics. *Proceedings of the 2004 American Society for Engineering Educational Annual Conference and Exposition, USA*, Session 2666.

[2] Siegel, P. H., Omer, K., Agrawal, S. P. (1997). Video simulation of an audit: An experiment in experiential learning theory. *Accounting Education 6*(3), 217-230.

[3] Li, T., Greenberg, B. A., Nicholls, J. A. F. (2007). Teaching experiential learning: Adoptions of an innovative course in an MBA marketing curriculum. *Journal of Marketing Education, 29*(1), 25-33.

[4] Wassenaar, D., Woo, D., Wu, P. (2009). A certificate program in computer forensics. *Journal of Computing Sciences in Colleges*. 24(*4*), 158-167.

[5] Thomsen, B. C., Renaud, C. C., Romans, E. J. Mitrofanov,)., Rio, M., Day, S. E., Kenyon, A. J., Mitchell, J. E. Retrieved March 1, 2010, from eprints.ucl.ac.uk/18955/1/18955.pdf

[6] Willis, K. V., Clerkin, T. A. (2009). Incorporating reflective practice into team simulation projects for improved learning outcomes. *Business Communication Quarterly. 72*(2), 221-227.

[7] Kolb, A. Y, Kolb, D. A. (2005). Learning styles and learning spaces: Enhancing experiential learning in higher education. *Academy of Management Learning & Education*, *4*(2), 193–212.