Proceedings of the 11th Colloquium for Information Systems Security Education
Boston University
Boston, MA June 4-7, 2007

Combining Theory with Practice in Information Security Education

Li-Chiou Chen and Chienting Lin, *Pace University, Member, IEEE*

Abstract – To meet the current industry demand for qualified security professionals, we need innovative courseware that can help students apply information assurance theory into practice. This paper describes our experience in designing hands-on information assurance courseware that addresses the current demand. In addition, we have presented a survey instrument to assess our design based on the contents of lectures, the contents of laboratory exercises, the relevance between the lecture and laboratory exercises, and the overall impact of the class on students. From the evaluation results of fifty students, we found that students generally agreed that they have learned better with the hands-on laboratory exercises. Given that many of the students we surveyed expressed interests in applying security in their respective domains, we believe that it is needed to start focusing on creating interdisciplinary IA courseware.

Index terms – Security Education, Hands-on Lab, Information Assurance Courseware

I. Introduction

Information security has become an importance issue for many organizations in different disciplines, such as banking, finance, and telecommunications. The annual CSI/FBI computer crime and security survey [1] has shown that information security has continuously been an top priority in many organizations. This trend brings a great demand for qualified Information Assurance (IA) professionals. A recent IDC survey [2] estimated that the number of information security professionals worldwide in 2006 has increased 8.1% over 2005, approximately 1.5 million. The number is expected to increase in the coming years. This demand has provided a great opportunity for academic programs in computer science and information systems. To meet the current tr[1]end, we need innovative courseware to train qualified security professionals.

The purpose of this paper is to provide our experience in designing information assurance courseware that combines theory with practice. Using well-designed hands-on laboratory exercises, we allow students to experience the technical details of what they have learned from information security lectures. We will discuss how we gather information and how we design the courses. We will also present a survey instrument used to collect feedbacks from students. We expect that our hands-on courseware design experience will be useful for other information security educators.

This paper includes five sections. Section two provides a framework for IA curriculum development and identifies the need for innovative courseware design. Section three describes the process, the difficulty and the requirements of designing hands-on IA courseware. Section four presents an evaluation instrument for assessing our IA courseware. Survey results from fifty students are presented and analyzed. Section five summarizes our contributions and suggests future works

II. A Framework for IA Curriculum Development

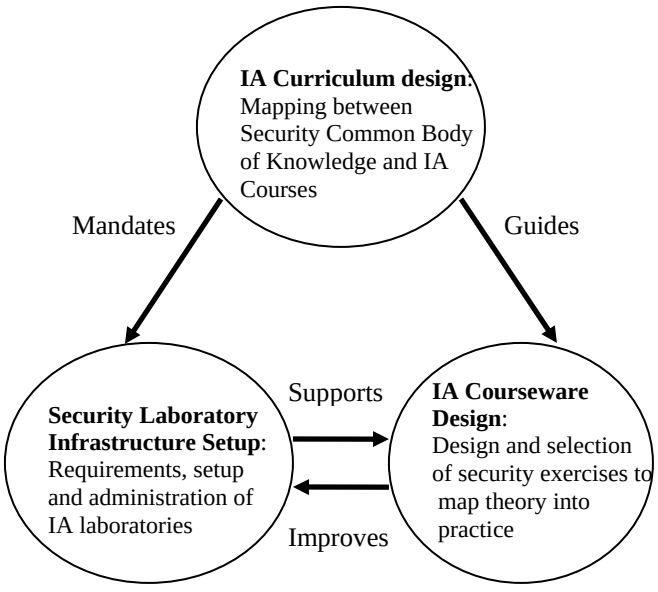

Figure1: A Framework for IA Curriculum Development

Information Assurance curriculum development can be categorized into three types of activities: IA curriculum design, security laboratory infrastructure setup, and IA courseware design, as shown in Figure 1. IA curriculum design is the basis for guiding IA courseware design, as

Both Li-Chiou Chen (lchen@pace.edu) and Chienting Lin(clin@pace.edu) are Assistant Professors in the Department of Information Systems in the Seidenberg School of Computer Science and Information Systems, Pace University.

well as for mandating security laboratory infrastructures needed to support the curriculum. Security laboratory infrastructure supports IA courseware development, while IA courseware development improves the planning and design of the security laboratory infrastructure.

A. IA Curriculum Design

The first task that IA educators face when teaching information security courses is to design a coherent and consistent curriculum. Previous IA curriculum development efforts have centered on deriving the course offerings through surveys or discussions with field experts [3, 4]. IA Curriculum should also consider existing government or industry best practice and standards [5] and identify security roles in organizations and their pertinent knowledge areas [6]. Most importantly, IA curriculum designers need to contemplate the integration of security course offerings into existing computing curriculum [7].

B. Security Laboratory Infrastructure Setup

The next major task for teaching IA courses is building security laboratory infrastructure to support security course offerings. Previous literature [6] has thoroughly discussed laboratory design, hardware and software options, and, most importantly, laboratory administration issues. Given the current trend of providing security education online, many researchers have started to develop "virtual lab" to support their IA courses remotely [8, 9].

C. IA Courseware Development

While current literature mostly focuses on security curriculum or laboratory infrastructure design, many IA educators and researchers have come to recognize that designing security laboratory exercises, i.e., the IA courseware, deserves more attention and considerable development efforts. A recent and complete listing of suitable security exercises can be found in a laboratory manual by Whiteman and Mattord [10]. At the same time, educational psychology models such as Kolb's Learning Cycle has been adopted to provide more effective security training [11].

While teaching IA courses with hands-on laboratory exercises, we found that it is difficult to combine appropriate laboratory exercises in the current available courseware with topics covered in our courses. The courseware often needs to be specially re-designed in order to meet specific learning objectives. Motivated by the lack of specific courseware to meet our demand, we have developed our own hands-on courseware in security courses, at both undergraduate and graduate levels.

III. HANDS-ON INFORMATION ASSURANCE COURSE DEVELOPMENT

Information assurance classes that combine hands-on exercises require the preparation of both regular lectures and laboratory exercises. We design the courseware in a way that the laboratory exercises could bring operational experiences to students in additional to regular lectures. The classes that we have offered so far are required courses for undergraduate students who study toward a minor in Information Assurance. These students are either Computer Science or Information Systems majors. We will discuss our courseware design from three aspects: information gathering, course structure and laboratory exercise design.

A. Information Gathering

Gathering up-to-date information for the courseware is very time-consuming due to the lack of appropriate textbooks and the rapid change of this field. Generally, instructors need two types of textbooks for teaching hands-on information assurance classes: those that cover principles with examples supporting the exposition and those that cover current tools and technologies. What we need in hands-on classes is the courseware that provides IA principles and supplements with related tools and technologies to show how the principles work in practice. At the time of writing the paper, only two textbooks that cover tools and technologies using step-by-step hand-on laboratory exercises [10, 12]. Nonetheless, they do not provide exercises along with contents on security principles that are suited for regular lectures. In addition, both security exploits and security technology advance at a very fast pace. According to CERT/CC, 5990 and 8064 security vulnerabilities have been reported in 2005 and in 2006, respectively. Textbooks alone simply cannot catch up with the rapid changes of this field. Because of these reasons, we collect relevant information from newly published papers and security publications from academic journals, open source community and security community. For example, SecTools.org's list of "Top 100 Network Security Tools" is very useful when we are looking for open-source security tools.

B. Course Structure

Each of our classes is consisted of a regular lecture and a hands-on exercise assignment. We include the hands-on exercises as a part of the weekly class although they can be organized as a recitation section if teaching assistants are available. For each week, we focus on one topic in the

area of information assurance. We have designed hands-on exercises for two courses: Overview of Computer Security and Network Security. In the Overview of Computer Security class, we cover basic topics such as public key and private key encryption, vulnerability assessment and application security. In the Network Security class, we cover specific network security issues such as network traffic analysis, network attacks, firewalls, and intrusion detection. All these topics are included in NSTISSI 4011 [13] and CNSSI 4013 [14], which are required by the National Security Agency to certify an institution as a National Center of Academic Excellence in Information Assurance Education (CAE/IAE).

Each of our classes is consisted of a lecture and laboratory exercises. The lecture introduces theories, concepts and current technology development. The laboratory exercises allow students to conduct hands-on exercises based our step-by-step instructions, which are contained in a single compressed archive for easy access. This compressed file includes an instruction document and the software or program codes needed to run the exercises. The instruction document is consisted of an overview of the technology used, step-by-step laboratory instructions, and discussion questions. After the weekly lecture, students are asked to download the compressed laboratory file from our server, to follow up the instructions for configuring software, and to investigate discussion questions asked in the lab instructions.

To tie together various topics taught in the class, we assign students a term project at the end of the semester. Students are allowed to pick a topic of their choice from a set of open research problems discussed in the classes throughout the semester. Each project has to tackle a security problem by conducting hands-on laboratory exercises designed by the students themselves. We have found that the term project serves as a great opportunity for students to apply their problem solving skills learned from this class. Our previous three classes have covered various project topics, such as a study on Wi-Fi security vulnerability, a study of peer-to-peer software security, and intrusion detection using Snort with BASE.

C. Laboratory Exercise Design

We design the laboratory exercises with four criteria in mind: relevance to lectures, affordability of laboratory setup, compatibility with the existing laboratory environment, and simplicity and portability of the exercises. Using examples, we explain the four criteria below.

1. Relevance to lectures

We select a set of laboratory exercises that are closely relevant to our weekly lecture topic in order to explore the weekly topic in operational details. This criterion allows students to gain hands-on experience from laboratory exercises about the theories or technology discussed in the lecture. For example, when firewall technology is introduced, the laboratory exercises include setting up a network-based firewall, designing firewall rules and testing firewall setting by exploiting the hosts inside the perimeter of the firewall protection. From setting up and testing a real firewall, students learn how important it is to setup appropriate firewall rules. The hands-on experience provides students with a more realistic view than lectures alone on protecting an internal network using firewall technology.

2. Affordability of laboratory setup

The affordability of laboratory setup is critical for running laboratory exercises. Our security laboratory is configured with a set of desktops, three servers and CISCO networking facility. The equipments are supported by a CISCO facility grant and a capacity building grant from Department of Defense for CAE/IAE. Since our budget for purchasing security software is limited, instead of adopting expensive commercial software, we have used mostly open-source security software or evaluation versions of commercial software. For example, we use Snort in exercises while we introduce intrusion detection systems (IDS). In this laboratory exercise, students are asked to monitor network traffic and to scan each others' hosts. By analyzing the network traffic and IDS logs, students learn how a signature-based IDS works.

3. Compatibility with the existing laboratory environment

We design our laboratory exercises to be compatible with a very simple laboratory environment, a handful of desktops within several Ethernet segments. The computers in the laboratory can be accessed externally through a Virtual Private Network connection. Currently, twelve desktops are connected to six Virtual LANs (VLAN) so that the desktops can be flexibly reallocated and more desktops can be added later. We develop the exercises in our security laboratory and create portable virtual environments using virtualization software, such as VMware. The environment setting is flexible enough so that most of our exercises can be duplicated in other computer laboratories in our university as well as most of the computer laboratories available in a college campus. For example, the network traffic signature analysis exercises require two computers in which one of them sends scanning traffic to the other and the other can detect and analyze the scanning traffic using an IDS and network traffic capturing software. Such exercise can also

be contained in a VMware file that simulates activities between the two computers.

4. Simplicity and portability of the exercises

We try to simplify the laboratory instructions and setup by packaging each exercise in a compressed file. In one single file, students will be able to find instructions, software needed and other related documents. We can then easily conduct the laboratory in another computer laboratory or assign students to run the laboratory exercises as homework assignments. We also use bootable Linux Live CDs, such as Knoppix or Ubuntu because of their flexibility. Students are able to conduct Linux-based exercises on Windows based PCs using these bootable CDs.

D. An Example

We usually design five to six exercises for a weekly topic, which is covered in one laboratory assignment. Typically, it takes a student about one and a half hour to two hours to finish a laboratory assignment. Appendix A is an example of a laboratory assignment that focuses on signature analysis using a packet capturing tool, Wireshark, and an open-source intrusion detection tool, Snort. The weekly topic in this lecture covers intrusion detection which discusses the definition of intrusion detection, types of intrusion detection systems, false-positives and false-negatives in intrusion detection and signature analysis using network traffic. The lecture runs about 2-3 hours depending on the length of the discussions during the class. Appendix A shows an overview of the lab assignment and two exercises in detail to illustrate our design. Since students vary in their technical skills, the lab session can run from one to one and a half hour, sometimes two hours.

IV. EVALUATION

In order to evaluate how effective our students think the courseware is, we solicited students' opinions using an anonymous questionnaire at the end of a semester. The purpose of the questionnaire is to assess how closely our hands-on exercises mapped to our lectures from students' point of view and if students have learned more about course topics after taking the laboratory exercises. We can then improve our courseware based on their opinions.

The questionnaire consists of questions in four categories: the contents of lectures, the contents of laboratory exercises, the relevance between the lecture and laboratory exercises, and the overall impact of the class on students. Each category contains four positive statements about the course. Questions were presented using a five-point Likert scale. Students were asked to rate the statement based on a scale from 1 (strongly disagree) to 5 (strongly agree). In addition, we collected demographics of our subjects. Table 1 is a summary of the demographics of the study participants and Table 2 is a summary of the results from 50 students in 3 different classes, taught by two instructors. Two of the classes are offered as Overview of Computer Security and the other is offered as Network Security.

Number of Participants	50
Number of classes	3 (one master class and two undergraduate classes)
Highest education degree completed	36% : High school diploma 50% : Professional, technical, or trade school diploma 10% : Associate's degree 4% : Bachelor's degree
Average age	32
Sex	78% : Male 22% : Female
Average years of working experience	6.9
Average years of IA work experience	1.9
Current use of security related computer applications or tools	24% : Never 22% : about once a month 20% : about once a week 24% : about once or twice a day 6% : three to five times a day 2% : more than five times a day 2% : no answer
Current general computer use	4% : about once a month 10% : about once or twice a day 14% : about three to five times a day 72% : more than five times a day
Availability of computer access	2% : at office/school 14% : at home 80% : both 4% : no answer

Table 1: Summary of demographics

Survey Item / Average / (Standard Deviation)	**Category average /Standard deviation**
Q1. The contents of the lectures improve my knowledge in information security/computer network security. 4.6 (0.6)	Lecture: 4.5 (0.6)
Q2. Each lecture has a well-designed theme in information security/computer network security. 4.5 (0.6)	
Q3. Each lecture has sufficient supporting course materials, such as handouts, slides, textbook materials, for me to understand and review the weekly topic. 4.7 (0.5)	
Q4. The contents of the lectures covers topics that I would like to learn in information security/computer network security. 4.4 (0.7)	
Q5. Each lab exercise can be finished within the designed lab hours (1 to 1.5 hours). 4.1 (0.8)	Lab/ Homework Exercises: 4.4 (0.7)
Q6. Each lab exercise has a theme in the area of information security or computer network security. 4.5 (0.7)	
Q7. Lab exercises stimulate my further interests in learning other security software or technology. 4.4 (0.7)	
Q8. The lab equipments are sufficient for running the required lab exercises. 4.5 (0.7)	
Q9. I have better understanding regarding the weekly topic after finishing the corresponding lab exercises. 4.4 (0.7)	Mapping between Lab/ Homework Exercises and Lectures:
Q10. I know better about putting the technologies or concepts/theories being taught in practice after finishing the related lab exercises. 4.1 (0.8)	
Q11. The combination of the lectures and lab exercises makes the class more interesting and informative than a class with only lectures. 4.7 (0.5)	
Q12. Lab exercises stimulate my further interests in learning the technology and theories/concepts behind the security software or security problems. 4.4 (0.7)	4.4 (0.7)
Q13. After taking the class, I am even more interested in the information security/computer network security area that I did. 4.3 (0.8)	Overall Assessment: 4.3 (0.8)
Q14. After taking the class, I am even more interested in having a career in the information security/computer network security area than I did. 4.1 (0.8)	
Q15. This class improves my knowledge and skills in the area of information security/computer network security. 4.5 (0.6)	
Q16. I will be interested in taking other security classes that blend in lab exercises with lectures. 4.4 (0.8)	

Table 2: Summary of results from the courseware questionnaire

A. Result Analysis

In general, students gave favorable evaluation of the three security classes. The averages of all questionnaire items are between 4.1 and 4.7 with standard deviations from 0.6 to 0.8. This result shows that students mostly either agree or strongly agree with the positive statement about the classes. Among the four categories, "lecture" (category one) has the highest average (4.5) and "overall assessment" (category four) has the lowest average (4.3). This result shows that students are satisfied with the contents of our lectures but are less certain about the overall impact of the classes on their career.

Both question 3 and 11 have received the highest average with the lowest standard deviation. This result indicates that students are satisfied with the course materials and enjoy the classes when the laboratory exercises are combined as a part of the class activities.

Questions 5, 10 and 14 have received the lowest average but with the highest standard deviation. This result shows that some students have difficulty finishing the laboratory on time, some are not sure about how to apply what they have learned into practice, and some are less inspired by the class in terms of pursuing a future career in information assurance. We are not surprised by these results. During the classes, we actually found a large

variation in students' ability to complete the laboratory exercises. Some students could finish the exercises earlier than the designed time frame and some needed more time. In addition, since we did not use commercial security software, students learned only the fundamental concepts on each topic but not the specifics of any commercial products. As to a future career on Information Assurance, students may come to the class with a different purpose. Some of them are working or majored in an application discipline, such as finance or criminal justice. They took the courses to gain a better understanding on security technology. They might not necessarily plan to work as security professionals but needed to deal with security problems in their own specific fields. Nevertheless, some of our students actually successfully secure positions in information assurance after taking these courses.

B. Implications of Our Results

Our survey results have three implications on information assurance curriculum development. First, we found that hands-on laboratory exercises allow students to understand the weekly course topic better than lectures alone. We would recommend IA educators to incorporate hands-on laboratory exercises into their courseware whenever possible. Second, we found that hands-on laboratory exercises make the course more interesting and informative to students. Students often raise questions whenever they encounter problems that prevent them from completing the exercises but they do not usually ask questions during a lecture. Third, interdisciplinary education between information assurance and an application field such as banking or criminal justice would be a future direction to pursue. From our survey, we found that students are interested in more hands-on security classes but do not necessarily want pursue a career in IA. Typically, these students are pursuing a career in an application field other than information security. Nevertheless, they need to know security technology and emerging issues related to their specific field. This career choice creates a demand for interdisciplinary education between information assurance and other application fields.

V. CONCLUSIONS

We have presented our hands-on courseware design that combines IA practice with theory. We have also described the process, the difficulties and the requirements for designing such courseware. Our experience should help IA educators in planning their IA courses and in bringing more interesting and informative learning environment to the students.

Our hands-on IA courseware has three unique features. First, each of our weekly hand-on lab exercise is a self-contained file consisted of instructions and tools needed. It is simple to setup the lab environment for both the instructor and the students. Second, the weekly course packages are adaptable in a limited budget and are portable to most computer laboratories in universities. Third, each weekly hands-on courseware is closely tied to a related security concept or principle covered in the lecture.

In addition, we have developed a sample evaluation instrument that measures students' feedbacks. Using this survey instrument, we found evidence that suggests students indeed feel that they learn better about contents of our weekly lecture after taking the hands-on exercises. Given that many of the students we surveyed expressed interests in applying security in their respective domains, we believe that it is needed to start focusing on creating interdisciplinary IA courses and courseware, e.g., security in trading or healthcare applications.

We would also like to further refine our evaluation instrument to include questions that address learning outcomes, such that we can improve our courseware to better combine theory into practice. Last but not least, we will continue to assess the effectiveness of our approach through a longitudinal study.

VI. REFERENCES

[1] L. A. Gordon, M. P. Loeb, W. Lucyshyn, and R. Richardson, "Computer Crime and Security Survey," CSI/FBI 2006.
[2] A. Carey, "Global Information Security Workforce Study" IDC October 2006.
[3] M. Dark and J. Davis, "Report on Information Assurance Curriculum Development," NSF Curriculum Development Workshop June 1st, 2002.
[4] B. Bogolea and K. Wijekumar, "Information Security Curriculum Creation: A Case Study," in 1st Annual Conference on Information Security Curriculum Development, Kennesaw, Georgia, USA, 2004, pp. 59-65.
[5] E. Crowley, "Information System Security Curricula Development," in 4th Conference on Information Technology Curriculum, Lafayette, Indiana, USA, 2003, pp. 249-255.
[6] M. E. Whitman and H. J. Mattord, "Designing and Teaching Information Security Curriculum," in 1st Annual Conference on Information Security Curriculum Development, Kennesaw, Georgia, USA, 2004, pp. 1-7.
[7] R. B. Vaughn, D. A. Dampier, and M. B. Warkentin, "Building an Information Security Education Program," in 1st Annual Conference on Information

[8] W. C. Summers, Bhagyavati, and C. Martin, "Using a Virtual Lab to Teach an Online Information Assurance Program," in 2nd Annual Conference on Information Security Curriculum Development, Kennesaw, Georgia, USA, 2005, pp. 84-87.
Security Curriculum Development, Kennesaw, Georgia, USA, 2004, pp. 41-45.
[9] V. Padman and N. Memon, "Design of a Virtual Laboratory for Information Assurance Research and Education," in National Colloquium for Information Systems Security Education Atlanta, 2005.
[10] M. E. Whitman and H. J. Mattord, Hands-on Information Security Lab Manual. Boston, MA: Thomson Course Technology, 2005.
[11] E. Crowley, "Experiential Learning and Security Lab Design," in 5th Conference on Information Technology Education, Salt Lake City, UT, USA, 2004, pp. 169-176.
[12] V. J. Nestler, W. A. Conklin, G. B. White, and M. P. Hirsch, Computer Security Lab Manual: Career Education, 2005.
[13] NSTISS, "National Training Standard for Information Systems Security (InfoSec) Professionals," NSTISS June 20 1994.
[14] CNSS, "National Information Assurance Standard for System Administrators (SAs)," Committee on National Security Systems March 2004.

VII. Appendix A: A Sample Lab Exercise Assignment

IT304 Internet and Network Security, Spring 2007

Topic: Intrusion detection

[Exercise I: Environment setup]
....
(This exercise asks students to setup software environment needed to conduct subsequent exercises.)
.....
[Exercise II: Capture packets using Wireshark]

This exercise will ask you to use one computer (your computer) to scan another (your partner's computer) and capture the network scanning traffic. One of the computers will conduct port scan using a tool called SuperScan. In the meantime, another computer being scanned will run a port listening tool to simulate the situation when a server running many services. In addition, this computer will use Wireshark to capture the scanning traffic.

1. Run the port listening tool on your computer.

1.1 Under the lab folder, click on attacker.exe.

1.2 Click on "ports" tab on the left panel. Check TCP box. Pay attention to what TCP ports will be scanned and click on OK.

1.3 Click on Start. Now, you can see the computer is listening on multiple TCP ports and is waiting for connections.

2. Use Wireshark to capture network packets from your Ethernet card.

2.1 Click on Windows Start, All programs, and Wireshark.

2.2 To capture a packet, click on "Capture" and "Start" on the menu bar.

2.3 You will see a small window called "Wireshark: Capture Options".

2.4 You need to select the Ethernet driver for your computer. Under "Interface", select the Ethernet card that this computer uses.

2.5 Make sure that the "Capture packets in promiscuous mode" box is checked. This box is usually checked by default.

2.6 Click on "OK" to finish the setting.

2.7 Now, you should see a small "Wireshark: Capture" window.

2.8 Your Wireshark is collecting network traffic. Now, wait for your partner (or another computer) to generate scanning traffic.

3. On a different computer (your partner), use SuperScan to scan the computer where you setup Wireshark. Follow the instructions below to use SuperScan:

3.1 Under the lab folder, click on SuperScan4.exe.

3.2 In Hostname/IP box, type in the IP address of your partner's computer.

3.3 Click on "Host and Service Discovery" tab to see what options are selected at this moment.

3.3 Click on "Scan Options" tab to see the default options.

3.4 Click on "Scan" tab back to the scan setup. To start scanning, click on the start button at the bottom of the screen. (the icon with a blue arrow)

3.5 The SuperScan window will show the progress of the scanning. Wait until the window shows "Discovery scan finished."

3.6 After the tool has finished scanning, click on "View HTML Results" to see the scanning report.

4. Copy and paste your scanning report below.
_____

5. Are the TCP opening ports consistent with the ones that the other computer listens using the port listening tool? __ Are the opening ports consistent with the ones you have known in Exercise I?_____

6. After the scanning is finished, on the Wireshark computer, click on “Stop” to stop the packet capturing.

[Exercise III: Analyze traffic signature using Wireshark]

1. Examine the packets captured by Wireshark. Look at only the packets sent from or sent to the scanning computer.
2. Filter out other packets by setup a filter. In the filter box, type (ip.addr eq your IP address) || (ip.addr eq scanning computer’s IP address).
3. Find an ICMP Echo from the scanning computer. How did your computer respond to the ICMP Echo?

_____

4. Check out the TCP packets from the scanning computer. Are there any common patterns among these TCP packets? Describe the common pattern below:

_____

5. What are the purposes of these TCP packets?

_____

6. How does the Wireshark computer respond to these TCP packets?

_____

7. Check out the UDP packets from the scanning computer. Are there any common patterns among these UDP packets? Describe the common patterns below:

_____

8. What are the purposes of these UDP packets?

_____

9. How does the Wireshark computer respond to these UDP packets?

_____

[Exercise IV: Capturing network traffic using Snort]

....
(This exercise asks student to capture scanning network traffic using Snort.)
.....

[Exercise V: Capturing intrusion patterns using Snort]

....
(This exercise asks student to analyze intrusion patterns using Snort.)
.....