Learning IT Security in a classroom setting has often been a challenging endeavor for both instructors and students alike. From our experience, traditional instructional methods like direct instruction and lectures though widely used and effective in most other areas still need to be augmented specially in the area of developing real world IT Security skills.

In this article, we shall propose an approach to augment traditional learning methodologies in IT Security called Honeynet Learning. This approach uses the honeynets as tools and resources to augment learning in both students and instructors alike.

This approach will incorporate the learning concepts that we feel are important to promote learning in IT Security namely discovery, feedback, and “real world” experience. Aside from this, we shall be illustrating a proposed methodology built upon these concepts that can be applied in a typical IT Security course.
We believe that Information Technology (IT) Security learning is an area that would benefit greatly with the integration of the honeynet (Spitzner, 1999). A honeynet is an advanced form of a honeypot. It is a security resource whose value is in its being probed, attacked, or compromised (Spitzner, 2002). Think of it as a computer’s “black box.” Anything happening in a honeynet is recorded and stored for future analysis therefore providing researchers and in our case, students, an opportunity to examine real live cases that they wouldn’t usually have access to.

Thus, the honeynet by its inherent nature as a data collection and data analysis tool could become a valuable if not integral resource for IT Security instructors for teaching and training their students. In fact, the honeynet could be viewed not only as a resource but better yet, as an opportunity for instructors to go beyond traditional instructional methodologies and present their students with a more situated and active form of learning.

SHELL-SHOCKED STUDENTS

“Learning is not a spectator sport” - Chickering and Gamson

Direct teaching and lectures have always been the most widely accepted instructional method (Kizlik, 2005). This mode relies on factual presentation of material in a direct and logical manner by the instructor. In this method, learning targets are usually very specific and already predefined before the course starts.

![Figure 1. A traditional model](image-url)
A typical IT Security lecture often begins with the instructor delivering a lecture that is taken from a reference book. Let’s say that in this instance, the lecture is about port scanning. Here the instructor identifies the tools used for this process. The instructor then proceeds to demonstrate each tool to the students and allows them to use the tools on each others in a “clean” lab environment. The process is then repeated for each subsequent lesson and culminates in a written or practical exam based on a “scenario” created by the instructor.

While traditional methodology is effective in teaching specific facts and basic skills, it still leaves us with a number of areas, essential to IT security, which cannot be addressed through lectures and direct teaching alone. From the point of view of IT Security practitioners, these essential areas are:

1. applicable scenarios;

2. problem-solving skills; and

3. feedback and interaction with colleagues.

These areas are in some ways not fully addressed by traditional methodologies because of a number of reasons that are usually characteristic of these methodologies:

1. highly dependent on the knowledge base and skill of the instructor;

2. students are generally passive and communication is generally one-way;

3. may not be effective to develop reasoning skills; and

4. lack of applicable scenarios.

Thus to stress our point, we feel that for students to fully benefit from IT Security education, traditional methodology should be augmented to include teaching of “real world” skills essential for would-be IT Security practitioners. By leaving their education with gaps, our fresh IT Security soldiers will be coming out half-baked which unfortunately, will leave them shell-shocked once they step into the beachhead of the IT Security war.
HONEYNET LEARNING CONCEPTS

“Give me a place to stand and with a lever I will move the whole world.” - Archimedes

So how does this all have to do with honeynets? Simply put, we will make our honeynet our lever for learning. It is a common assumption that “knowledge” means “information” but we must realize that true knowledge implies understanding. This is the underlying principle of what we are proposing: that for students to learn it is imperative to understand the nature of threats rather than just memorizing information about them.

Thus by fostering understanding, we shall be giving our students the tools that will let them adapt to “real world” scenarios rather than just spoon feeding them with facts and trivia. This is where Honeynet Learning comes in.

Honeynet Learning is a discovery and scenario-based method of learning about IT Security threats and issues that incorporates the use of Honeynets and its data into the study program. This method is built around 3 basic tenets:

![Figure 2. Tenets of Honeynet Learning](image)

**Figure 2.** Tenets of Honeynet Learning
Learning Should Be Discovery or Problem Based

Discovery or problem based learning challenges students to “learn to learn.” Introducing gaps, incongruities, or disturbances provides the students an important stimulus and motivation for learning (Ellis, 1938). By posing problems instead of just lectures, the students are encouraged to discover the underlying nature of a topic and not just be content on superficial information gathering.

Learning Should Be Feedback and Discussion Based

Pask’s Conversation Theory (Pask, 1975) stated that learning occurs through conversations about a subject matter, which serve to make knowledge explicit. We believe that by creating a learning environment that focuses on discussion and through the honeynet, which we found as a superb feedback tool for learning, we shall effectively reinforce the knowledge gained through the course.

Learning Should Be Situated and Experiential

“To facilitate perception, realistic environmental settings should be used in instructional materials.” - Information Pickup Theory (Gibson, 1977).

All we’re basically saying here is that in order to be able to gain “real world” skills, we should be using “real world” scenarios. The practice is in no way new. It is the reason why medical professionals have their internships in actual hospitals and not just in their school laboratories.

In order to learn, we must be immersed in the situation. Unfortunately, IT Security students don’t have the luxury of internships but by adding honeynets into the equation, we are hopefully providing them with this very important component of learning.
THE VIRTUAL HONEYNET HOSPITAL

“Hmm...I guess it must be a Denial of Service...”

To construct our methodology, we have borrowed the concept of rounds from medical training. This concept of rounds pertains to doctors and students going through different cases together as a teaching and learning endeavor. In these rounds, each of the students have their own cases to analyze and discuss with the group and their instructors.

The problem of applying this methodology per se to IT Security is based on the lack of actual cases that could be used for study. With the introduction of the honeynet as our resource we are effectively introducing our own “virtual hospital” where IT Security students can take their cases from and for the class to do their “rounds” in.

We have constructed a variant of this methodology based on the Honeynet Learning concepts. Our methodology is illustrated in Figure 3.

Figure 3. The Honeynet Learning methodology
Introduction

Each course will begin with a problem and scenario analysis by the instructor. This will be a demonstration of what the students will be doing as they progress through the course. Think of it as an initial “observation” phase where they are given a taste of what’s to come and given an idea of how to approach the problems they will be given in the subsequent steps.

The important thing here is that the scenario presented must be simple enough as not to give away solutions to the problems that will be posed to each group in the later step but engaging enough to pique the students’ interest. The instructor must emphasize that the scenario are actual cases taken from the Honeynet thereby accentuating the feeling of relevance of what they are studying. The students must also be reminded that after this course, they will be expected to present a similar analysis of an actual case to the class.

Problem Posing

This step poses a very important challenge to the instructor. The problem or problems given to each student are by default “real world” because it was taken from our honeynet. This may range from anything from a web server attack to reverse engineering of a malware (Holz, Marechal, & Raynal, 2006) depending of course on what’s appropriate to the students’ level of understanding. This already gives our cases a significant edge from traditional learning. But it is not enough to just get any random “real world” case from our honeynet and give them to the students. It is important for the instructor to choose the right problems.

Choosing the right problem for each group or student is essential for our methodology to be effective. An effective problem must first engage the students’ interest and motivate them to probe for deeper understanding. It is preferred if the instructor knew something of the background of their students in order to choose a more appropriate problem. Some questions that the instructors might want to ask themselves before choosing a problem from our honeynet could be:
What is the case about?

What are some of the potential learning issues I want to address with the case?

Are the issues central enough to the case for me to use this case?

Can I easily modify the case?

How difficult or obscure are the issues in the case?

Will these be issues my students will care about?

Is the case open-ended enough for students to go beyond fact finding?

What do I see as possible areas for investigation?

Is the case too short or too long for the time I have available?

What sorts of learning resources might be needed for this case? Are they accessible?

Ideally, students should be given individual problems. But depending on the size of the class and the number of possible scenarios from our honeynet, it might be practical to group them at first. But essentially, the smaller the group, the better (Rios, 2002).

Research and Analysis

This is where the fun starts. Each group or students are given the appropriate “start up” tools and resources for him to start analyzing their problem. Data from the honeynet where the cases were taken from should be liberally provided. The students should be provided with a disk image and a pcap file for starters. The instructors are advised to go to the Honeynet Project website and refer to their Honeynet Challenge for more information on what resources to be given and extracted from their honeynets. Of course, aside
from our honeynet data, the Internet and reference texts should also be considered as valuable reference resources.

Data analysis tools should also be provided. Readily available tools such as “The Coroner’s Toolkit (TCT)” should be considered. Maybe the instructor could even consider providing the students with a shared Walleye account (ROO) though we advise against it if you haven’t disconnected your honeynets for this exercise.

From the initial demonstration by the instructor (see step 1), the students should already have an idea on the techniques and tools to use for his analysis. The students should also be encouraged to use (or even develop) any other techniques or tools that they think would be relevant to the problem they are analyzing. They must be given free reign on how they will approach the analysis to solve their problems for this not only increases understanding but promotes creativity (Langley, Simon, Bradshaw, & Zytkow, 1987) as well.

**Generation of Partial Hypothesis**

As analysis progresses, the students will slowly form a hypothesis based on their findings. Keep in mind that it is not necessary to form a full hypothesis right away. This should be done in parts and are subject to discussion and feedback after each “round.” For example, if the students think that in their case, the attacker used a “WINS Buffer Overflow attack” vulnerability to gain control of a computer, they should present this partial hypothesis for discussion before integrating it to the final hypothesis.

**Discussion and Feedback**

Cooperation from all members of the class should be necessary to effectively work through a good problem (Duch, 2001). After each Analysis and Partial hypothesis step, the whole class will have a discussion and feedback session to complete each “round.” Each of the student or groups will present a progress report.
The reports could initially be as simple as identifying and describing the nature of the compromise to the class. After a few meetings, the reports would then eventually progress to more specific aspects of the case such as how a scan was made? What specific vulnerability was used? And so on.

It is not necessary though for the reports to take the form of a narrative since we are aiming for a discussion. In fact, the instructor must encourage the students to pose questions to each other. If the students presenting have a certain bottleneck in their analysis, they may ask the class for advice since other students in the class may have encountered the problem already. The instructor, in their capacity as experts must mediate the discussion by posing their own “leading” questions and/or views to make sure the discussion is pointed towards a productive direction.

**Presentation of Final Hypothesis**

The final hypothesis is basically an aggregate of all research and analysis done throughout the class “rounds.” Each student or group will be required to submit a paper and a short demonstration of their hypothesis. We recommend that this paper be composed of the following sections:

![Figure 4. Proposed final hypothesis template](image-url)
The hypothesis will obviously start with a **problem and issue identification**. In this case, the students will not only have to state the main problem but break down the problems into their component issues, which they used to solve the main problem.

The **conceptual framework** is essentially the concepts involved in solving the issue. For example if a student determines that the scenario involved a DDoS attack using the UPnP vulnerability, a part of the section would obviously be reserved for the discussion on the principles of UPnP, SSDP, and DDoS.

The **resource review** is related but not similar to what is commonly termed literature review in research. In our case, the resource review is a description of all relevant resources that the students used in determining the solution to their given problems. This should include all materials including a description of the IDS alerts, disk images, websites, tools and reference materials used. This is included so that students looking at an old final hypothesis paper could recreate the solution implemented by the authors of the said paper.

The **investigation and scenario walk-through** is the body of the paper. This part is where the solution to the problem is presented. This could be a step by step recreation of a compromise, a reverse engineering of a malware or even documenting the discovery of a new worm. As we’ve indicated earlier, this all depends on the problem given, the important thing is, the walk-through should be comprehensive and all the steps done in solving the problem should be documented. This should not be a problem after going through several rounds of progress reports already.

No research is without a **conclusion and a recommendation** so there is not much need to further elaborate on this. We suggest though that special attention be given to the recommendation part since this is what gives the research its value. For example, if a student was able to discover a new worm using the honeynet, aside from just describing its nature and reverse engineering its code, a recommendation on how to stop the worm would give the work much more relevance and value to the community.
Assessment

This step was initially called “exam” but since exams are not the “end all” of student performance measurements we coined it “assessment” instead. As stated, there are a number of ways instructors could assess their students’ performance using the Honeynet Learning methodology. Some of these are:

1. evaluation of student performance in Partial Hypothesis presentation (and discussion);
2. evaluation of the Final Hypothesis paper;
3. peer evaluation (whole class) and Group evaluations (if students works in groups); and
4. final “real world” case based exam taken from Honeynet.

We propose that a large part of the assessment score be taken from the first two products, the Partial Hypothesis presentations (and discussion) and the Final Hypothesis paper since these are the actual product of the “rounds” that the students made. Peer and group evaluations are often good indicators in terms in the cooperative and interpersonal aspect of learning but more often than not, in the authors’ opinion are often slightly deviated to the more “extroverted” personalities. The final “real world” case based exam though important should only be a validation mechanism of the assessment done using the first two products.

CONCLUSIONS AND RECOMMENDATIONS

“Are we clear?”
“Crystal.”

-Jessep and Kaffee (Jack Nicholson and Tom Cruise), A Few Good Men

It is our belief that through Honeynet Learning, we shall be able to augment lecture based IT Security education. Through this system we hope to bridge theoretical learning with the very practical world of IT security by providing our students with real world experience and skills that are important, if not essential for IT Security practitioners.
By using honeynets to provide situated problems and by incorporating “rounds” as a discussion and feedback mechanism, we hope to provide a system that will adhere to the principles that we believed are important to make good IT Security practitioners.

To reiterate the concepts of this article, these principles are:

- learning should be discovery or problem based;
- learning should be feedback and discussion based; and
- learning should be situated and experiential.

These principles are the basis of the Honeynet Learning methodology. This methodology as we’ve discussed follows a similar pattern to medical rounds. Aside from being able to handle and discuss real world cases of their own, the methodology is also geared to expose students to each others cases and viewpoints to bring about a broader perspective of the IT Security field as a whole. This methodology as discussed has the following steps in which the middle three steps are the “round” mechanism:

1. introduction;
2. problem posing;
3. research and analysis;
4. generation of partial hypothesis;
4. discussion and feedback;
5. presentation of final hypothesis; and
6. assessment.

In the future, we hope to do some further research on the following aspects of Honeynet Learning:

- provide criteria for choosing problems / cases from the honeynet;
- create a categorized honeynet case “pool” with all accompanying resources for instructors to use in their classes;
refine the assessment procedures to be used in evaluating the students;

provide a more comprehensive logistical description for the course; and

provide a post-course continuing education mechanism.

Finally, as an ending to this article, we sincerely hope that Honeynet Learning would someday find its way to IT security education. As IT Security continues to evolve, let us not forget that education and learning must evolve with it.

References


Note

Mark Ryan del Moral Talabis is now at Secure-DNA Consulting, Honolulu, Hawaii.