J. L. Hernández-Ardieta, et al., "An Intelligent and Adaptive Live Simulator: A new Concept for Cybersecurity Training", *9th Future Security Conference*, 2014.
NICS Lab. Publications: https://www.nics.uma.es/publications

AN INTELLIGENT AND ADAPTIVE LIVE SIMULATOR: A NEW CONCEPT FOR CYBERSECURITY TRAINING

Jorge L. Hernández-Ardieta[1], David Santos[1], Pascual Parra[1], Juan E. Tapiador[2], Pedro Peris-López[2], Javier López[3], Gerardo Fernández Navarrete[3]

[1] *jlhardieta,dsesteban,pparra@indra.es*
Indra, Avda De Castilla 2, 28830 San Fernando de Henares, Madrid (Spain)

[2] *jestevez,pperis@inf.uc3m.es*
University Carlos III of Madrid, Av. de la Universidad 30, 28911 Leganés, Madrid

[3] *jlm,gerardo@lcc.uma.es*
University of Malaga, Malaga (Spain)

Abstract

The rapid rate of change in technology and the increasing sophistication of cyber attacks require any organization to have a continuous preparation. However, the resource and time intensive nature of cybersecurity education and training renders traditional approaches highly inefficient. Simulators have attracted the attention in the last years as a potential solution for cybersecurity training. However, in spite of the advances achieved, there is still an urgent need to address some open challenges. In this paper we present a novel simulator that solves some these challenges. First, we analyse the main properties that any cybersecurity training solution should comprise, and evaluate to what extent training simulators can meet them. Next, we introduce the functional architecture and innovative features of the simulator, of which a functional prototype has already been released. Finally, we demonstrate how these capabilities are put into practice in training courses already available in the simulator.

Keywords: Cybersecurity, Cyberdefence, Education, Training, Simulation.

1 INTRODUCTION

The rapid rate of change in technology and the increasing sophistication of cyber attacks require that any organization ensures continuous preparation and training of their staff to effectively prevent, detect and respond to cyber threats. However, specialised education and training are resource and time intensive, as it must consider the complexity of the problem faced, and may have undesirable impacts on staff availability if extended over long periods of time.

The most common approach followed nowadays by organisations is to pursue industry professional security certifications. However, these certifications usually mean expensive fees for training and maintenance of the professional certificate. Contents are not tailored to the organisation's needs, not are able to address the specific problems and cyber threats applicable to their context. Besides, contents are quickly outdated with respect to the state of the art of technology and latest trends in cyber attacks. Some certifications do not include sufficient hands-on training in the curricula, so they are hardly able to offer continuous uptake of technical expertise and perfection.

On the other hand, we find a large number of efforts towards solving the practical aspects of cybersecurity training, mainly hands-on exercises in either academic labs or at the industry. These labs provide a technological environment where the student can be trained in defensive and offensive techniques, sometimes in a classroom and instructor fashion, others accessing remotely with no human support. In general, they are good at dealing with the practical aspects of IT education and training, but still pose

some limitations, such as the inflexibility of the model and the resource constraints when classroom approaches are mandatory. If not, the main limitation is that student monitoring, guidance and problem resolution are hardly possible.

Tabletop exercises are also a relevant effort towards cybersecurity training and awareness. A tabletop is designed to test the theoretical ability of a group to respond to a situation that changes in response to their actions. The exercise is usually aimed at testing cooperation in addition to readiness to respond to crisis and emergency situations [1]. A clear benefit of a tabletop exercise is the ability to put people into hypothetical extreme situations without causing any real effect. However, because of this it is unable to train and evaluate practical aspects or achieve immersive realistic training in a way similar to that we find in the real world.

Another option that is gaining momentum is what is called a cyber defence exercise (CDX) [2]. In CDX several stakeholders are grouped together to collaborate (or compete) in a single scenario where attacks and defences take place, having to deal technically with the incidents but also learning how to better prevent and react in collaborative manner against grave situations. The benefits of CDX are varied. They support highly complex exercises consisting of multiple stakeholders and a wide array of possibilities for the underlying IT infrastructure. They enhance intra- and inter-organisational coordination capabilities as well as competitive attitudes (role playing). Also, the scenarios loaded are realistic, using real products and technologies and generating manual attacks on existing networks.

On the contrary, this sort of exercises implies some significant disadvantages. They are not designed to cover varied scenarios, so a holistic training is not possible. The exercises are hardly reproducible without a tremendous effort. The exercises involve a complex coordination, scheduling and execution, and the design, deployment and configuration are resource consuming as well. They are not intended for individual or flexible training. Student monitoring and adaptation to heterogeneous skills are hardly achievable, and assessing the scoring in competitive scenarios is very complex without the involvement of expert instructors and heavy out-of-band control mechanisms.

The need for having a cost-effective training environment to undertake continuous improvement of technical skills and competences in evolving and challenging scenarios is obvious. Next section reviews the concept of simulation for training, with a special focus on cybersecurity. Some of the primary properties that any cybersecurity training solution should comprise are enumerated, and we discuss to what extent training simulators can meet them. Section 3 presents the solution that Indra is currently developing. We analyse the main building blocks, the functional architecture and some of its innovative features. Finally, some conclusions are given in section 4.

2 SIMULATION FOR CYBERSECURITY TRAINING

Simulators have long been considered a key ally to support cost-effective training programmes in different civil and military contexts. A simulator can be defined as a software/hardware tool that models the state and internal properties of the simulated system, being able to produce observable effects and properties similar to those of the real system (performance, interactivity, etc.).

The main advantages of simulation for training are:

- Achieve complex pedagogical objectives supported by mature technology.
- Offer high availability compared to that provided by the simulated systems.
- Provide rich scenarios and situations for the student, even extreme situations that would otherwise be risky and expensive.

- Lower TCO compared to using the simulated systems.
- Timescale manipulation is possible, adjusting the synchrony and delay of actions as a response to the student's behaviour.
- Manipulation and control of the environmental effects and progress of the exercise is possible.

According to the LVC (*Live*, *Virtual*, *Constructive*) classification for simulators [3], these work on four dimensions (personnel, systems, commands and environment) as shown in the next Fig.

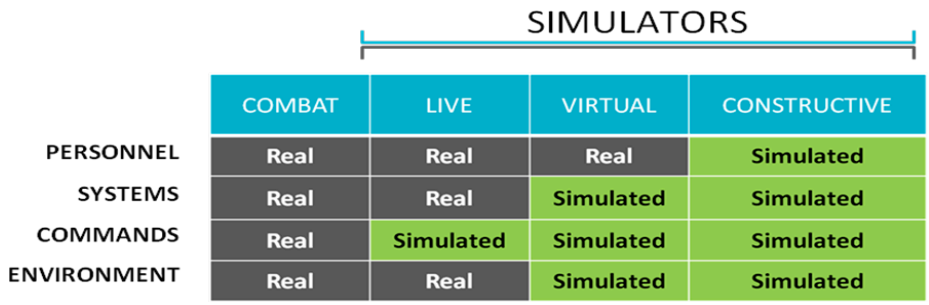

Figure 1 LVC classification

Live simulators are those amongst the three the ones that provide the maximum cognitive and physical reliability. However, they also have the same disadvantages that we find in any training platform based on the real, physical elements. Live simulators pose the same risk for the student, do not reduce significantly the costs, and can hardly implement mechanisms to control the exercise at will. In [4], a thorough survey and classification of different simulators for security education, training and awareness is provided. Most of the simulators reviewed would fall in the constructive and virtual categories, whilst others would fall in the live category. For example, tools like as DETERlab or RADICL were designed to support CDX or experimentation activities.

Thanks to the nature of the cyberspace as well as the virtualization technology [5], we observe that we can construct Live simulators with an adequate cost-benefit balance, making the most of live simulation (realism) at the time that the limitations of live simulation are overcome. Fig. 2 summarises the benefits obtained from live simulators for cybersecurity training derived from each of the dimensions.

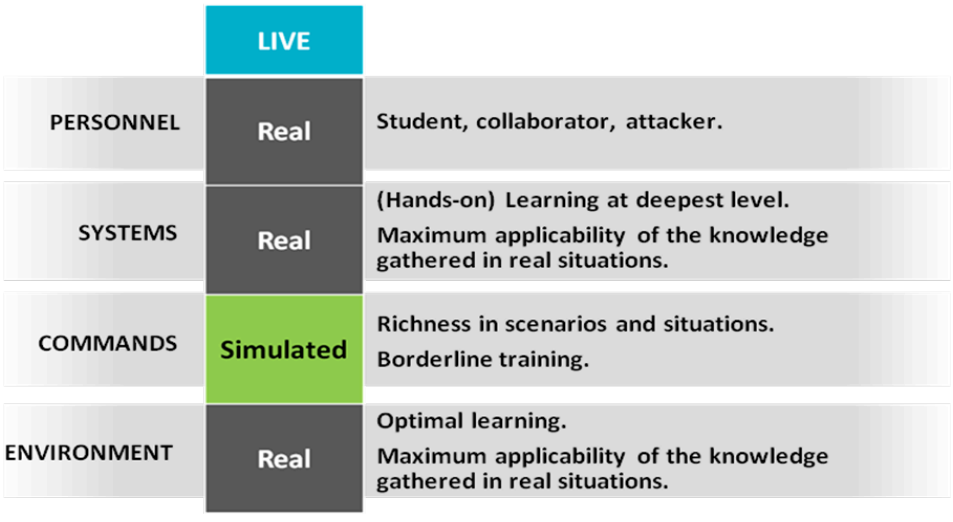

Figure 2 Benefits of Live simulators

In general terms, a live simulator for cybersecurity training shall meet the following properties:

- **Realism**. The simulator shall provide exercises that use real information systems and communication networks that reproduce real-world scenarios with real-time feedback and operation. The student shall be able to learn from hands-on experiences, using and managing multiple defensive/offensive security solutions.
- **Growth**. The simulator shall have the capability of defining, creating and setting up new training sessions and exercises with little or no technical nor procedural constraints, and according to the evolution and changes in the technology and the threat landscape.
- **Flexibility**. The access to the simulator shall be as less restrictive as possible, allowing the student the remote access with little or non technical limitation regardless where and from when they access.
- **Role oriented**. The simulator shall have the capability of adapting the training dynamics to the role of the student (strategic, tactical, operational).
- **Usability**. The simulator HMI and functionality shall be easy to use.
- **Size**. The simulator shall be capable of reproducing large networks and scenarios with hundreds and even thousands of assets.
- **Security**. The simulator shall offer a high level of security, such as isolation from production environments, access control, use of secure software engineering for product development, etc.
- **Reproducibility**. The simulator shall allow the student to repeat, pause, resume and restore the exercises at any time.
- **Richness**. The simulator shall have the capability of incorporating a wide array of scenarios, techniques, defensive and offensive tools, attackers' profiles, configurations etc.
- **Pedagogical**. The simulator shall embed a variety and effective learning processes and pedagogical strategies, such as observational learning (play automated exercises), trial and error approaches (active attitude, capability to undo actions and take different courses of action, etc.), quantitative scoring system and gamification mechanisms to encourage competitiveness and self-improvement.
- **Supervision**. The simulator shall include the capability of supervising, monitoring and assessing the student's actions and performance, using either automated means (preferably) or human-based mechanisms.
- **Adaptability**. The simulator shall include the capability of adapting to the level of difficulty of the training to the student's skills and performance, including dynamically.
- **Control**. The simulator shall include the capability of automatically (preferably) or manually controlling the execution of the exercise to unblock certain situations, execute alternative paths, know the progress and state of the exercise, etc.
- **Guidance**. The simulator shall include the capability of providing guidance and tips to the student to help him during the training activity to enhance the learning process.
- **Customizable**. The simulator shall include the capability of easily adapting and customizing the exercises to the student needs, without the need to stick to predefined scenarios and exercises.

- **Intelligence**. This property relates to the overall artificial intelligence of the solution that enhances many of the other features, such as having the capability to automatically and dynamically propose new challenges to the student, reinforce certain attitudes, improve the adversary skills for highly proficient students, etc.

3 THE ADVANCE SIMULATOR FOR CYBERSECURITY TRAINING

This section includes background information about the research and innovation programme to develop the Indra simulator, details about the simulator conceptual architecture and building blocks, as well as some insights about its intelligent automated attack capabilities.

3.1 Project background information and objectives

The Indra advanced simulator for cyberdefence experimentation and training (simulator from now on) has been conceived as a solution for the technological experimentation and continuous training in cybersecurity, providing an advanced environment for improving capacities and skills to detect, react and respond to cyberattacks. The simulator is a solution under development within the framework of a research and innovation programme, and where two Spanish Universities collaborate (University Carlos III of Madrid and University of Malaga). The project started at the end of 2011, and will finish at the end of 2014.

The Indra simulator has been designed to enhance five skills:

- **Prevention**, including vulnerability assessment; enforcement, optimization and system patching.
- **Detection** and **reaction**, covering aspects such as network and system secure configuration; monitoring and security management (SIEM, Firewall, IDS/IPS, network probing …).
- **Forensics analysis**, including hard disk (FAT, NTFS, ext2, ext3, ext4) and memory analysis of both Windows and Linux O.S.; collection and centralised custody of evidence; and report generation.
- **Attack**, covering exploration and identification of targets, vulnerability analysis; exploitation and consolidation.

The simulator will support four types of exercises, each of them specifically aimed at training a particular set of skills. *Forensic analysis*, where the student has to undertake a methodological forensic analysis of a certain attacked system; *Cyberdefence*, where the student has to defend a target system from automated attacks launched by the simulator; *Cyberattack*, where the student has to achieve a set of predefined objectives by implementing cyberattack techniques against a specific target system; *Cyberwarfare*, which include cooperative/competitive scenarios where two teams are confronted, and each one has to defend their own system while attacking the opposite's one.

Indra has recently released a beta version of the simulator for demonstration purposes and that includes several exercises in forensic analysis.

3.2 Functional architecture

In this section we provide a brief overview of the functional architecture of the simulator. In particular, the next Fig. depicts the conceptual architectures for the four types of exercises supported. As can be seen, virtualisation is used to load the target system, i.e. the set of information systems and communication networks that have to

be analysed, defended or attacked, depending on the type of exercise, as well as any other component needed, like the cyber attack platform.

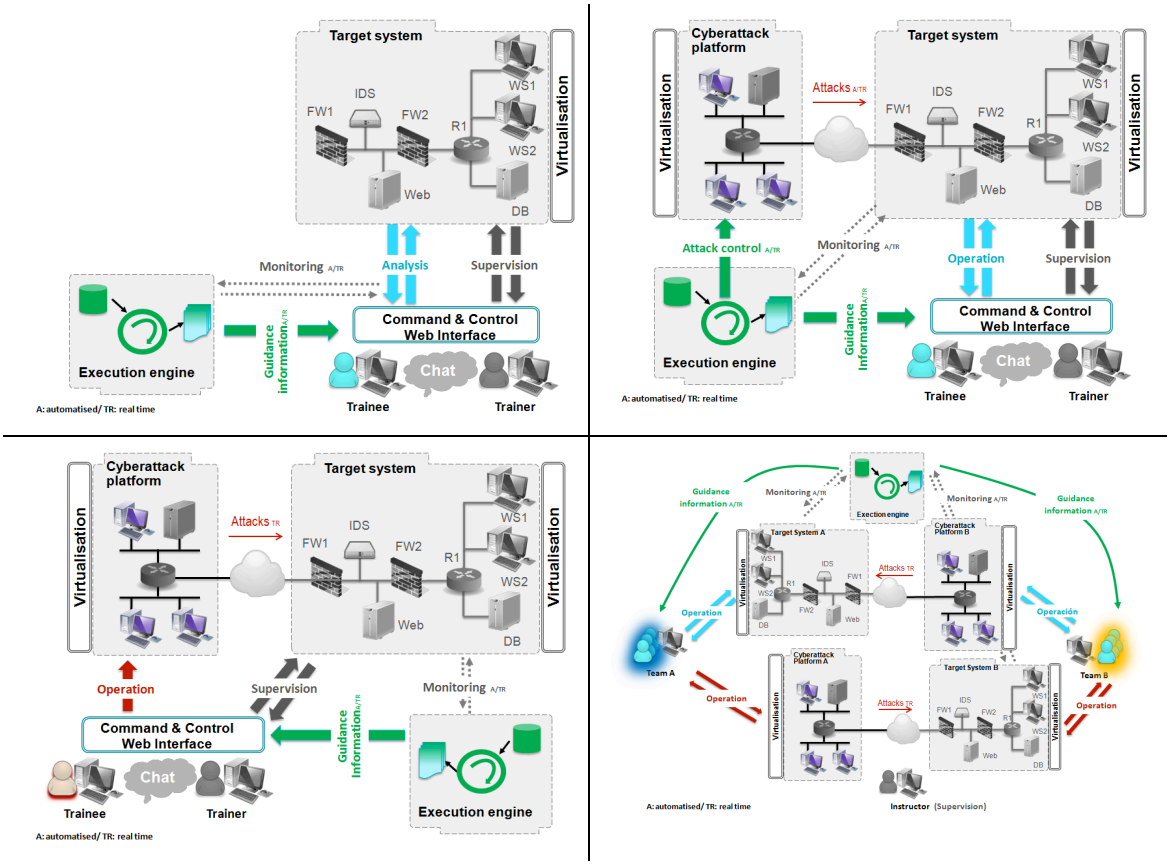

Figure 3 Conceptual architectures

The main building blocks of the simulator are shown in the next Fig.

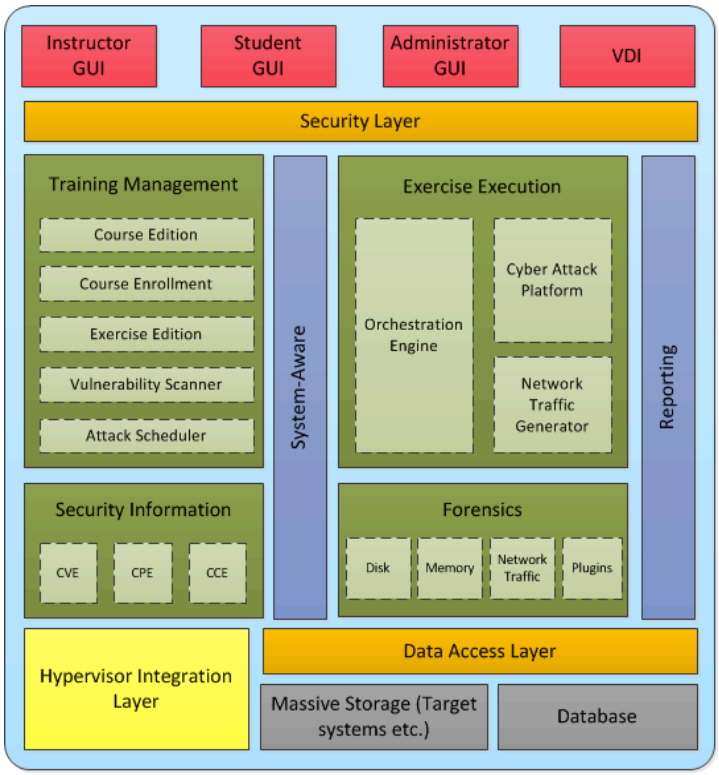

Figure 4 Building blocks of the simulator

There are two large functional areas reflected in the Fig. above. The *Training management* comprises all components to create and manage training courses and exercises. It includes a *vulnerability scanner* developed adhoc for the simulator, and which is capable of performing in depth vulnerability assessment of complex networks and systems, analysing not only published services but also internal services running in each workstation and server. The *Attack scheduler* is explained in the next section.

The other relevant building block is the *Exercise Execution*, which includes three components paramount for executing live simulations. The *Orchestration Engine* is the heart of the simulation, as it controls the evolution of the exercise, detects whether the objectives of the exercise are being fulfilled, monitors the performance of the student and is able of producing recommendations and tips in the case that such a performance decreases below a predefined threshold. On the other hand, the *Network traffic generator* is the component in charge of producing the legitimate traffic inside the virtual network in a manner that makes a cyberdefence or cyberattack exercise close to real environments. The *Cyber attack platform* is explained in the next section.

3.3 Automating attacks in an intelligent manner

As part of the simulator's architecture, a component for deploying controlled attacks into a virtualized environment has been designed. It is focused on automating the process of exploiting vulnerabilities or breaches in a virtualized network where students have to learn how to react under an attack scenario. To facilitate the process of modelling and executing attacks in a defensive environment, different modules have been developed which provide functionality at three levels: assessment, management and execution of attacks.

The *Cyber Attack Platfform* (CAP) provides a front-end component for executing attacks without the need to know the low level implementation details. The *Exploit Manager* implements a set of methods related to the management of modules used by the CAP. The *Attack Scheduler* or *Expert System* is in charge of analysing and deciding the best routes to compromise a host marked as an objective.

Fig. 5 shows the component-level architecture for the attack capabilities of the simulator. The CAP consists of a web service that receives a set of actions to be performed though a modified version of Metasploit[1]. Besides the execution of attacks, the CAP also analyses the result of these actions, providing an evaluation of the successfulness of the attacks launched. The Exploit Manager is a service that is in charge of adapting Metasploit modules for its use in the CAP. This process includes the normalization of the different modules stored in the database of Metasploit and the generation of CLIPS rules associated to these normalized modules.

In an attack scenario, where students take on the role of defenders, there are many different kind attacks that can be launched in an automated way, but many of them are not needed in order to reach the pedagogical objective of the exercise. Indeed, attacks have to been orchestrated in such a way that each single action is selected with a purpose. For example, compromise a system that will grant access to an isolated network where the objective is located. This is the aim for which the ExpertSystem has been designed. This module provides a set of attack paths that drives to the objective, but the criteria for deciding which path is better for enhancing the learning experience is left to the instructor during the definition and creation of the exercise.

The Expert System uses a connectivity map (a representation of the reachability of network hosts) and information regarding each host (platform, public vulnerabilities, etc.) to generate attack paths that can be performed using the CAP to reach the goal

[1] http://www.metasploit.com/

stated by the instructor. This component uses a representation in CLIPS of each Metasploit module available in the exercise, the connectivity map and the information related to each single host involved in the scenario.

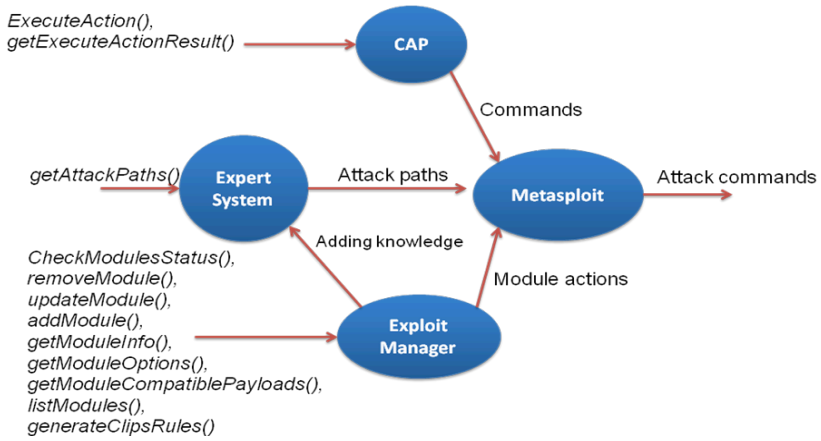

Figure 5 Component-level architecture

4 CONCLUSIONS

The evolution of the technology and the threat landscape require that any organization ensures continuous preparation and training of their staff to effectively prevent, detect and respond to cyber threats. However, current approaches lack of the necessary properties to ensure a continuous, intensive, effective and economically feasible learning. To this end, simulators have proved to be a key ally for training and experimentation. This paper has enumerated the set of properties that any training simulator should comprise. In addition, we have presented the main features and capacities of a novel simulator for cybersecurity training that Indra and its academic partners are developing. The current beta version of the simulator is promising and has attracted much attention from several stakeholders, so we expect to release new versions with further functionalities in the near future this year.

ACKNOWLEDGMENTS

This work has been funded by the Spanish Ministry of Economy and Competitiveness under the INNPACTO 2011 programme, Plan Nacional de Investigación Científica, Desarrollo e Innovación Tecnológica 2008-2011, ref. PT-2011-1593-390000.

REFERENCES

[1] Dowell, J. (1995). *Coordination in emergency operations and the tabletop training exercise*. Le Travail Humain: A Bilingual and Multi-Disciplinary Journal in Human Factors, 58(1), pp. 85-102.

[2] White, Gregory B.; Dietrich, G.; Goles, T. (2004). *Cyber security exercises: testing an organization's ability to prevent, detect, and respond to cyber security events*. Proc. of the 37th Annual Hawaii International Conference on System Sciences.

[3] DoD Modeling and Simulation (M&S) Glossary (1998). DoD 5000.59-M, DoD.

[4] Pastor, V.; Diaz, G.; and Castro, M. (2010). State-of-the-art simulation systems for information security education, training and awareness. IEEE EDUCON 2010.

[5] Andel, T. R.; Stewart, K. E.; and Humphries, J. W. (2010). Using Virtualization for Cyber Security Education and Experimentation. Proc. of the 14th Colloquium for Information Systems Security Education.