The UWF Cyber Battle Lab: A Hands-On Computer Lab for Teaching and Research in Cyber Security

Chris Terry, Angelo Castellano, Jonathan Harrod, John Luke, and Thomas Reichherzer
Department of Computer Science, University of West Florida, Pensacola, FL, USA

Abstract - *With a dramatic increase in cyber threats over the last decade, government and industry alike have recognized the pressing need to combat the ever growing cyber attacks on networks and systems. Educational institutions play an important role in researching technology that improve resiliency of systems as well as growing a workforce that understands cyber security challenges and can study and combat cyber attacks. The Computer Science Department at the University of West Florida (UWF) has built a Cyber Battle Laboratory to support undergraduate and graduate education, faculty research and public/private partnerships. Faculty and students can freely experiment with methods of attacks, detection and prevention in a controlled and isolated environment without affecting the campus network or the Internet. The lab is equipped with state-of-the-art technology to assist faculty in reconfiguring the environment for instructional and research purposes. It has been successfully used for classroom instruction and outreach activities at UWF.*

Keywords: cyber security; computer networks; virtualization, educational technology, laboratories

1 Introduction

The increasing attacks on systems and networks over the last decade disrupt our daily life and threaten the operations of public and private sector organizations. Constantly in the news are stories of attacks to businesses, universities, and government systems. The Government Accountability Office reported that the number of cyber threats increased by 680% from 2006 to 2011 with hackers attacking the integrity of systems and networks to gain access to private data and disrupt services for personal and political gains [1]. According to a recent report by Norton, the damage to consumers world-wide due to cyber attacks is estimated to be $113 billion in 2013 [2]. The escalation of hacker attacks on our systems continues to be a major concern to businesses and governments that have invested in recent years significant amount of resources to harden system security and train their workforce to deal with the barrage of cyber attacks we experience. Educational institutions have stepped up to the growing need for IT professionals with cyber security background by offering specialized degree programs and certifications to students and professionals seeking to advance their career. In the U.S. alone the number of IT programs that specialize in cyber security has increased substantially over the past 5 years addressing needs in the public and private sector [3].

To address the workforce needs in the Northwest Florida region in cyber security, the Computer Science Department at the University of West Florida (UWF) has developed undergraduate and graduate specializations that combine traditional core areas in computer science with topics in cyber security including system and network security, digital forensics, cyber warfare and gaming. To support the new programs and faculty research, a new laboratory has been constructed that offers state-of-the-art network and computer systems to build large-scale computer networks and computing environments for experimentation.

The remainder of this paper is organized as follows. The next section describes our motivation for building the UWF Cyber Battle Laboratory (CBL) as well as ethical concerns that arise when students are exposed to methods of cyber attacks and malware. The paper then describes the infrastructure of the CBL detailing the emulation of an independent computer network and systems for experimentation before discussing hacker and support software tools for demonstrating cyber attacks to students. The paper concludes with a discussion of challenges, related work in cyber security education and future outlook for the cyber battle lab.

2 Motivation and Ethical Concerns

As part of a long-term teaching and research effort in cyber security, the Computer Science Department has established a new computing lab that creates its own network infrastructure disconnected from the campus network and the Internet. The lab is designed to provide students an interactive learning experience allowing them to solve practical, real-world problems to complement theoretical concepts discussed in classroom and textbooks. It supports lab exercises, capstone projects and thesis research, competition for students in cyber security as well as outreach programs offered to a broader audience in the regional community to spark interest in cyber security and foster new partnerships with business and industry. The cyber lab provides special software tools, pre-configured virtual computing environments and network services, as well as tutorials for instructors to demonstrate

cyber threats through viruses, worms, botnets, and a variety of man-in-the-middle and denial-of-service attacks.

In an effort to ensure that malware remains within the confines of the cyber lab, the lab's network infrastructure is completely isolated from the campus network. In addition, all workstations in the lab have been configured to limit access to data from local machines or the network by disabling all USB ports and removing CD drives. Any file transfer from the external world to the lab must be done through a special podium desktop computer that restricts access to files on computers in the lab to designated IT personnel. When students are given access to the lab they are instructed on the proper use of the laboratory and the potential danger in either bringing outside equipment into the lab or removing data from the lab. The United States Military Academy takes a similar approach with their Information Analysis and Research Laboratory, describing it as the IWAR Range, and instructing students to treat it the same way as they would treat any live fire weapons range [4]. Because security topics taught in the laboratory include attacks and penetration testing, one concern is ensuring that courses also cover the proper ethical uses for the tools the students are being exposed to. Just as it would be unthinkable for a cadet to remove a loaded weapon from a firing range to practice outside the range, the same mentality must be fostered in students when thinking about the tools used in the laboratory for attacks.

For exploring the ethics of computer security, a good example is the story of Randal Schwartz, an engineer working at Intel, who performed unauthorized penetration testing against their network and was eventually prosecuted [5]. While it is important that students are properly briefed on the importance of not using the tools they are exposed to outside the lab environment, a broader ethical discussion may be worth saving for the end of the course. Locasto and Sinclair have noted that an ethical discussion at the beginning of the course would “lack detail” and “focused more on emotional argument rather than informed debate” [6]. Students of the UWF CBL receive special instructions at the beginning of each course that gives them access to the lab. However, these instructions are put in a broader legal and ethical context at the beginning of the course to raise concerns for harm that the methods may cause to others and themselves should they be applied outside the lab.

3 The Cyber Battle Lab Infrastructure

The next section describes the configuration of computer workstations and servers in the lab and the physical networks that support cyber security experiments. The current lab has been constructed as a pilot lab to A) gain experience with hardware resources and virtualization software for simulating networks and B) predict resource needs to scale-up the lab's emulated wired and wireless computer networks for more realistic experimentation. It serves as a blue-print for building an expanded version of the lab in the summer of 2014.

3.1 Workstation & Server Environment

The pilot lab provides seats for 24 students that may be assigned to 12 computer workstations in teams of two for lab exercises. The workstations are equipped with dual monitor to provide better visualization of different virtual environments and two network interface cards each to connect the workstations to an experimental and a management network. The workstations run Windows 7 Enterprise as their host operating system with VMware Workstation 9 for virtualization of different machines. A workstation connects with the first network interface card (NIC) to the management network for general lab management services such as authentication and file sharing. VMware Workstation running within the host operating system is configured to use the second NIC installed in the system to connect to the experimental network. Figure 1 illustrates the configuration of the guest and host operating system and the separation between management and experimental network. The next section describes how the virtual environment and the host machine connects to two physical networks.

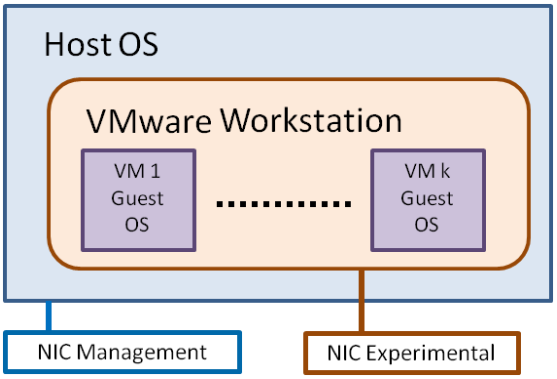

Figure 1. Workstation Network Connections.

In addition to the creation of two independent physical networks, the lab uses VMware Workstation to separate the experimental computing environment from the host environment. VMware Workstation runs virtual machines that are part of the various cyber experiments in the lab, while the host machine joins a general computer lab that supports centralized user authentication, network file systems, file sharing, and more. Each virtual machine executed within VMware Workstation implements a specific computing environment for launching or monitoring cyber attacks or defending against attacks emanating from a remote environment. Virtual machines may also be used to study strengths and weaknesses of operating systems or specific software application such as PDF viewers with known security weaknesses. Virtual machines may also be used to subject students to certain environments where malware has affected their systems to study how users respond to malware on their computer system or simply give users an opportunity to experience malware on a computer system without being harmed.

The lab includes two servers, one R210 II PowerEdge server equipped with an Intel Xeon E3 Quad Core processor and 8 GB of RAM purchased from Dell and one custom built 24 core AMD Opteron system with 64 GB of RAM, deployed with VMware ESXi. The R210 II PowerEdge server provides virtual servers for the management network to facilitate basic lab management and student file storage through a network file system. The custom server provides a virtualized lab environment on the experimental network that can be easily reconfigured to support a wide variety of research and educational activities with a minimal upfront investment in equipment. The VMware servers allow the multiple operating systems and network configurations to be simulated without physically reconfiguring the lab environment.

Using software from the open source Quagga project [7] the custom server runs several virtual routers to emulate large, interconnected wide-area networks. Each router executes within a single Linux server to emulate a network node within a wide-area network. Details of the wide-area network emulation and the physical network configuration follow below.

3.2 Wide-Area Network Simulation & Physical Network Configuration

In an effort to setup a more realistic setting for experimentation, the lab was designed to provide an accurate snapshot of a portion of the Internet infrastructure and a diverse set of emulated networks and hosts. We created a wide-area network that replicates parts of the Florida Lambda Rail education network, Internet Service Providers (ISPs), corporate networks (e.g. Google), and three Internet peering points including Equinox Chicago, Telix Atlanta, and NOTA Miami. Links between network nodes are mapped to Virtual Local Area Networks (VLANs) in the physical network discussed below. The virtual routers deployed in the emulated network implement common routing protocols such as the Boarder Gateway Protocol (BGP) and the Open Shortest Path First (OSPF) for routing data packets throughout the entire emulated network. Using published information from the Internet, the lab uses the same IP addresses used by the ISPs, corporate networks and Internet Backbone Peering Points to create the illusion for students and researchers to experiment with the actual Internet. Figure 2 gives a high-level description of the emulated network implemented by the lab.

In addition to the virtualized network, the lab implements network services such as Domain Name Services (DNS) for name resolution in corporate networks, universities, and ISPs as well as Dynamic Host Configuration Protocol (DHCP) to assign machines joining different networks automatically the corresponding IP addresses of the joined networks. Workstations in the lab may join specific ISPs, corporate or university networks as needed for implementing different attack scenarios or to collect network traffic data for analysis.

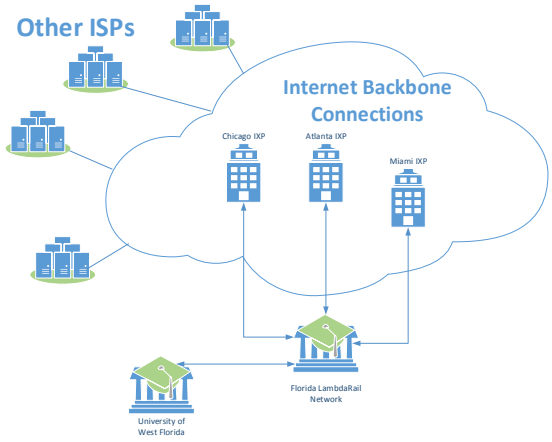

Figure 2: Simulated Wide-Area Network

The lab is designed to run a multiple well known services, including the DNS and TLD root servers, well known Web sites such as *google.com*, and corporate networks running Linux and Windows servers. This provides a familiar environment for students and researchers to use that accurately mirrors the real world Internet infrastructure. This infrastructure is designed to work in conjunction with additional virtual routers and hosts that can be run for individual experiments and classroom activities.

The physical network consists of a total of 3 switches, one layer-3 and two layer-2 switches. Each workstation connects to both layer 2 switches with their corresponding NICs to join the management and experimental network implemented by the switches. The R210 II PowerEdge server and the custom-built server connect to the layer-3 switch, which connects to the experimental network and management network switch. Traffic within the management network and experimental network is kept separate through VLANs implemented by all three switches. The custom-built server runs virtual routers on virtual machines that also use VLAN's to implement links between routers. **Error! Reference source not found.** Figure 3 shows the physical network configuration in the current CBL.

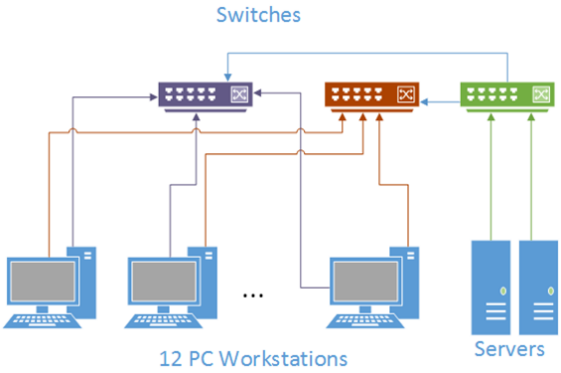

Figure 3: Physical Network Layout

VLAN tagging is used to allow the experimental network interface on the lab workstations to be able to run virtual machines on multiple networks simultaneously giving students and researchers the ability to join different networks with their virtual machines as if they were users on those networks or hackers that have successfully penetrated those networks.

The creation of a management and an experimental network serves two purposes. First, it ensure that the lab provides basic network services such as centralized account management via Active Directory and file sharing services needed for distributing virtual machines to workstation. Second, the separation ensures that malware is not affecting the host computers or the management network needed to run day-to-day lab operation and provide access to the simulated environments. Keeping the experimental and management network separate also gives instructors and researchers the power to refresh the lab after an experiment is completed or reconfigure the lab for an alternate experiment by simply starting and stopping virtual machines running virtual services in the network as needed. The following section discusses the tools and pre-configured virtual environments and tutorials that are available for teaching and research purposes.

4 Tools and Resources for Cyber Research & Education

CBL provides a number of software tools, customized environments and tutorial resources allowing users to demonstrate attacks, collect data from attacks or even implement their own attacks. The software tools implement widely known man-in-the-middle attacks that exploit weaknesses in network protocols and services. The tools are written in C using the raw socket interface available in a Linux environment to bypass existing protocols and create customized data packets for an attack.

In its current configuration, CBL implements the following attack methods:

- TCP SYN Flood
- DNS Query Flood,
- ARP Reply Flood,
- DNS and ARP Cache Poisoning.

These attacks have been discussed widely in the literature [8-12]. For space reasons, the paper will focus on a single attack method implemented for the CBL that exploits an ARP cache poisoning strategy combined with a DNS cache poisoning to re-route traffic to a fake Google server that runs on the hacker machine. Figure 4 shows the steps a hacker may take to redirect traffic to his own machine.

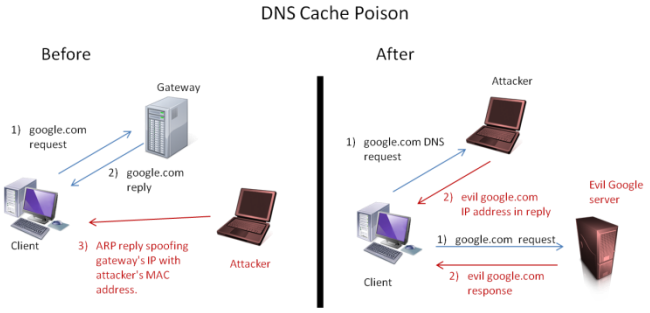

Figure 4: ARP Cache Poisoning attack to redirect traffic to a fake Google server.

The attacks are implemented on a virtual machine from where they can be deployed into any network. Figure 5 shows what happens on a lab workstation before and after the attack is executed. Note that the original Google server is a server that is replicated in the simulated computer network (the server only serves the home page for the Web search) on a Google corporate network and DNS queries are properly resolved by root and top-level DNS servers available in the network.

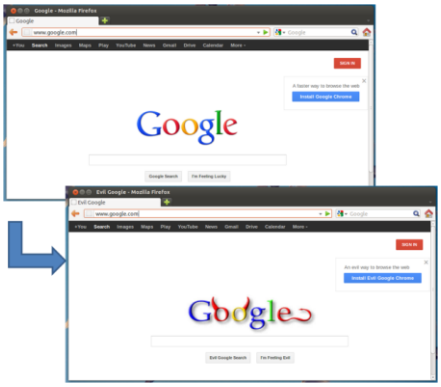

Figure 5: Google Web page as seen by a client before and after the attack.

The majority of software tools created for the CBL have been fully integrated into a Web application that implements a simple dashboard for launching attacks and performing various monitoring services. This dashboard is designed for instructors to control experiments in the lab for educational purposes. Besides attacks the dashboard also allows instructors to control startup of certain applications on the lab workstations such as Wireshark [13] or a Web browser to demonstrate remotely to users the successful execution of the attack or the content of certain data packets. The Web application is deployed on a virtual machine joining the network that is being studied for network attacks. Figure 6 shows a screenshot of the Attack Panel of the dashboard with an ARP Cache Poisoning attack executing.

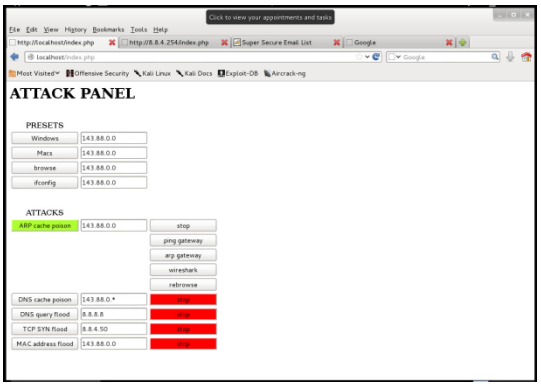

Figure 6: Attack Panel of the dashboard for launching attacks and remote controlling lab workstations.

To enable the dashboard to remote control applications on lab workstations, it uses a custom-built software installed on the virtual machine running the dashboard to send commands to the lab workstation via a UDP socket. Each workstation has the corresponding receiver software installed that listens for incoming commands from the dashboard to either open a Web browser, launch Wireshark, or run other visualization tools helping students understand changes in the environment that are illustrating the attack being studied.

All attack methods, fixes, and monitoring services are fully documented in a Wiki that instructors may access from the CBL podium desktop computer, to assist them with demonstrating cyber experiments in the lab, step-by-step.

5 Discussions

The CBL has been used for the first time in a cyber security class in the fall of 2013 and is currently being used in outreach activities. Students of the class last fall performed various lab activities to investigate network architectures and services to which the instructor exposed them. Students were also able to launch attacks and develop and implement defense methods. Finally, students were able to participate in a Red-team vs. Blue-team competition as a culminating project for the class. The hands-on experiments in the CBL environment was well received by students and the instructor of the class. Feedback solicited from participants of the lab showed that students had a good grasp of the security concepts such as man-in-the-middle or denial-of-service attacks because they were able to relate them to experiments they conducted in the class.

Building the software tools that implemented the various attack methods for CBL presented a number of development challenges for the programmers. When an attacker sends a spoofed DNS reply to a victim's DNS query, the spoofed DNS reply must arrive to the victim before its DNS server delivers a DNS reply back to the victim. Additionally, the DNS reply must contain a correctly matching DNS transaction ID and source port field or otherwise the victim's machine will declare it as invalid and discard the reply. Guessing the transaction ID or the source port information is not feasible as there are too many possibilities. However, by successfully completing an ARP reply flood to the victim's machine, all traffic will be re-routed to the hacker's computer and so any DNS query can be captured by the hacker to extract the transaction ID and source port information for generating a spoofed reply. And by pinging computers in a network, the attacker can extract a victim's valid MAC address to be used in subsequent ARP reply flooding. In multiple experiments run in the lab, our software tools implemented for the CBL have a 100% success rate in executing the cyber attacks named above. They create the basis for developing future attack, defense, and monitoring methods for the lab.

The current CBL supports 12 workstations that can be used by students working in teams of two. It simulates a small but realistic network environment by virtualizing routers and network services. Since the lab uses VMware workstation to virtualize network nodes and servers including DNS, file, Web, directory, mail servers and more, the entire environment can be easily recorded and archived via VMware snapshots. This allows for the network to easily be preserved and reset after various cyber attack experiments have been conducted giving users the needed flexibility to allow for changes to occur as caused by malware without suffering from permanent damages to the network and its services. The next step in the evolution of the CBL is to expand its hardware resources significantly so that the lab can replicate additional peering points, ISPs, corporate networks as they exist on the real Internet making the space more realistic for experimentation. Funding has been secured to include a total of 40-60 servers similar in their configuration to the custom-built server that would allow a total of up to 1000 virtual machines to be executed simultaneously implementing various network resources on an emulated large-scale network.

Most importantly, by creating a realistic environment of real-world services, the lab provides a suitable space for students to learn about cyber security threats. It has the capability to safely host demonstrations of attacks targeted at consumers and end-users, such as phishing attacks, which can be demonstrated against recognizable services that people use, such as banking Web sites. Students majoring in Information Technology can learn about such attack methods and how to defend systems and networks, while students from other disciplines can experience the effects of such cyber attacks and learn about best practices to avoid becoming a victim.

To present date, we are not aware of similar efforts to ours that create autonomous, fully-functional networks with support tools for automatic experimentation and management. The majority of projects discussed in the literature describe a small-scale environment with few machines deployed to examine specific network topologies and services [14-17]. Our lab offers a flexible environment through the virtualization of network routers and services to create wide-area networks linking corporate networks, ISPs, and educational institutions as they exist today on the Internet together in a single network. This environment allows for hands-on cyber experimentation giving students and researchers the opportunity to study cyber attacks and

methods of monitoring and prevention. With the additional hardware resources to be deployed this summer and the implementation of more sophisticated attack methods, the UWF CBL will be creating an environment that allows for realistic cyber experimentation and the development of new technology to monitor threats and better defend against them.

6 Conclusions

We present in this paper the design and implementation of a cyber security lab that plays an active role in cyber security education and research at UWF. The lab provides a safe environment for faculty and studens to experiment with cyber threats and learn how to detect and defend against possible attacks on systems and networks. The cyber lab has been used for the first time last fall semester by students of a cyber security class to explore widely used methods for studying weaknesses of systems and experiment with a number of cyber attacks playing the role of both an attacker and defender.

The initial use of the lab for classroom activities has shown the effectiveness of using special lab environments for cyber security education and research. The lab allows instructors to demonstrate live attacks on systems and networks to their students and discuss methods to defend against and trace the attacks giving students much needed practical experience. It allows faculty to customize networks and setup experimental environments for collecting data and testing new methods for monitoring and defending attacks. The lab built in the summer of 2013 is now being significantly expanded to create larger networks and allow for more realistic experimental settings to drive research and engage students in cyber security at UWF.

7 References

[1] United States Government Accountability Office. (2012). *Cybersecurity: Threats Impacting the Nation*, GAO-12-666T. [Online]. Available: http://www.gao.gov/products/GAO-12-666T.

[2] M. Merritt, and K. Haley. (2013). "2013 Norton Report", Symantec Corp. [Online]. Available: http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013.

[3] W. A. Conklin, R. E. Cline, and T. Roosa, "Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors," in *Proceedings of the 2014 47th Hawaii International Conference on System Sciences*, pp. 2006 – 2014, 2014.

[4] J. Schafer, D. J. Ragsdale, J. R. Surdu and C. A. Carver, "The IWAR range: a laboratory for undergraduate information assurance education," *Journal of Computing Sciences in Colleges*, vol. 16, no. 4, pp. 223-232, 2001.

[5] T. Wulf, "Teaching ethics in undergraduate network security courses: the cautionary tale of Randal Schwartz," *Journal of Computing Sciences in Colleges*, vol. 19, no. 1, pp. 90-93, 2003.

[6] M. E. Locasto and S. Sinclair, "An Experience Report on Undergraduate Cyber-Security Education and Outreach," in *The Second Annual Conference on Education in Information Security (ACEIS 2009)*, Ames, 2009.

[7] K. Ishiguor, "Quagga Software routing Suite." [Online]. Available at: http://www.quagga.net.

[8] S. McClure, J. Scambray, and G. Kurtz, Hacking exposed: Network security secrets and solutions (6th Ed.), New York, NY: McGraw-Hill Co., 2009.

[9] A. Harper, S. Harris, J. Ness, C. Eagle, G. Lenkey, and T. Williams, Gray hat hacking: The ethical hacker's handbook (3rd Ed.), New York, NY: McGraw-Hill Co. 2011.

[10] D. Kennedy, J. O'Gorman, D. Kearns, and M. Aharoni, Metasploit: The penetration tester's guide. San Francisco, CA: No Starch Press, 2011.

[11] C. Schuba, J. Krsul, D. Kearns, and M. Kuhn, "Analysis of a Denial of Service Attack on TCP" in *Proceedings of the 1997 IEEE Symposium on Security and Privcacy*, Lafayette, IN: Purdue University, 2011.

[12] M. Simpson, K. Backman, and J. Corley (2011). *Hands-on Ethical Hacking and Network Defense*. Boston, MA: Course Technology.

[13] Wireshark: The World's Most Popular Network Protocol Analyzer. [Online]. Available: http://www.wireshark.org.

[14] M. Micco and H. Rossman, "Building a cyberwar lab: Lessons learnied teaching cybersecurity principles to undergraduates," in *Proc. of 33rd SIGCSE Tech. Symp. Computer Science Education*, Northern Kentuck Convention Center, February, pp. 18-22, 2002.

[15] P. Mateti, "A virtual environment for IA education," in *Proc. of the 2003 IEEE Workshop on Information Assurance U.S. Military Academy*, West Point, NY, pp. 17-23, 2003.

[16] R. T. Abler, D. Contis, J. B. Grizzard, and H. L. Own, "Georgia Tech Information Security Center Hands-On Network Security Laboratory," in IEEE Transaction on Education, Vol. 49, No. 1, February, 2006.

[17] S. Standard *et al*., "Network reconnaissance, attack, and defense laboratories for an introductory cyber-security course," in *ACM Inroads*, Vol. 4, Issue 3, pp. 52-64, September, 2013.