Toward an Engaging Hands-on Environment for a Beginning Networking and Security Class

Lopamudra Roychoudhuri
Computer Science, Angelo State University
San Angelo, TX 76901, USA

ABSTRACT

This paper describes an active learner-centered environment for an introductory computer networking and security class using a lab classroom. The classroom makes effective use of virtual machines running on workstations, real devices in a locally connected network/security lab, and a dedicated but Internet-connected subnet, to discuss and explain complex concepts of computer networking, offensive and defensive security. The objective of the class is to demonstrate that offensive security techniques, such as hacking and penetration testing, are 'fun' and intriguing, but defensive security practices, though rigorous and detail-oriented, effectively address the issues discussed in offensive security. The three parts of the course, networking, offensive and defensive security, thus complement one other to provide a comprehensive picture to the students.

Keywords: Offensive security; Defensive security; Cyber security Education; Course Design.

1. INTRODUCTION

Students learn by doing [8]. A current trend of cybersecurity training is discussion of offensive security, 'a proactive and adversarial approach to protecting computer systems, networks and individuals from attacks' [27]. One of the biggest hurdles in cybersecurity education is effective teaching of offensive security. Offensive security is intriguing and fun to students, at the same time providing invaluable insight into the vulnerabilities and loopholes of computer and networking systems. The challenge is to create proper environments in order for students to freely, *but safely*, conduct hands-on experiments on cyber-attacks and 'hacking' techniques.

Defensive security, on the other hand, is about identifying and closing down the loopholes as much as possible. One needs to be rigorous and detail oriented in this process. Ideally, real devices, such as switches, routers and firewalls on a real network, should be used for students to experience actual configuration methods that implement the theory into practice.

In the light of the above, the contributions of this paper are as follows.

Effective Hands-on 'Playground'. We describe an innovative active learning environment for a beginning networking and security class. The classroom, designed with help from the university Information Technology team, makes effective use of virtual machines running on workstations, real devices in a locally connected network/security lab, and a dedicated but Internet-connected subnet, to discuss complex concepts of computer networking, offensive and defensive security.

Immersion Learning. The class has been implemented in two formats – an undergraduate semester long class and a workshop for professionals. In each case, students immerse into many hands-on experiments and learn by doing. As a foundation, students study the TCP/IP protocol suite [7] and capture underlying packet transmissions using Wireshark [28], a real-time tool that analyzes the protocol layers. Next, students play with intriguing yet potentially harmful offensive security techniques or 'attack' scenarios, such as reconnaissance, backdoor, IP-spoofing and password cracking, using Linux virtual machines running on their Windows workstations. Kali Linux [10], a penetration testing platform, is used as the 'attacker', and Ubuntu Linux [24] as the 'victim'. The virtual environment provides invaluable experience of 'hacking', but at the same time, ensures that the attacks stay safe inside a workstation and are not transmitted across network. Students then study Denial-of-Service (DoS) and conduct a DoS attack inside the classroom that demonstrates how easy it is to create a powerful attack. The attacks are confined inside the class subnet without affecting the rest of the university network. Lastly, students configure real security devices, such as switches and firewalls that are part of a locally connected network/security lab, which effectively demonstrate preventative measures of defensive security to thwart such attacks.

Complementary Components. The three parts of the course, networking, offensive and defensive security, thus complement one other to provide a comprehensive picture to the students.

The paper is organized as follows. In section 2 we discuss background and related work. Section 3 describes the course details. In section 4 we discuss the lessons learned. In section 5 we conclude and discuss future work.

2. BACKGROUND AND RELATED WORK

Traditionally cybersecurity education [1], [29] has focused on defensive security, that is, security goals of Confidentiality-Integrity-Availability (CIA) and the Plan-Protect-Respond cycle for security management [3]. Of late, offensive security has emerged as a new trend of security training, spearheaded by offensive-security.com [19] that provides Kali Linux as the penetration testing platform to conduct attacks on computer systems, network and Web applications to find vulnerabilities, and a considerable amount of accompanying trainings, certification and services. Metasploit [13], a similar penetration testing platform is from rapid7.com [21] that has also gained popularity. Many training materials can be found online [20].

Offensive security as a formal cybersecurity education method has gained traction of late [5], [11], [14], [22] where courses have been developed at universities to allow students perform penetration testing and exploits in controlled lab environments.

Our course is distinct from these courses in two ways. Many of these courses have pre-requisites that the students come prepared with before taking the mentioned course [22]. In contrast, our semester long course has no pre-requisite, as it is a

course taken by students of varied majors. We start at building a computer science and networking foundation before we can delve into the details of security. For the workshop, the attendees are intelligence instructors from an air force base with a varied set of technical skills. Similar foundation material needs to be discussed as background in this class as well.

Second, the above papers mention only one angle of training, either defensive or offensive security, but not both. In contrast, our course shows both sides, and how defensive security, when properly implemented, can successfully mitigate the attacks demonstrated in the offensive security part of the course.

3. COURSE DETAILS

3.1 Structure and Audience

This course is taught in two formats. It is a semester-long undergraduate course that has been offered in the Fall term over past four years. It is a required course in the certificate of Cybersecurity Technologies, offered by the Computer Science department, and in a Cybersecurity minor, offered by the department of Security Studies and Criminal Justice in the College of Arts and Humanities. Thus students from all backgrounds attend this course. Hence it is essential that a good foundation of computer science, such as number systems and Linux, and networking background is created, before we can delve into the bits and bytes of security.

In addition, a workshop has been designed for instructors and administrators of a local air force base, and has been delivered twice each summer for past two years. The workshop material has been created as a concise version of the undergraduate course material, consisting of the same module structure. Though this audience is significantly different from our undergraduate students, the attendees come with a vastly diverse set of expertise and technical backgrounds. Hence a similar foundation material is necessary as the first module.

3.2 Objectives, Modules and Exercises

Two main student learning objectives of our course are (1) to demonstrate understanding of network security terminology and concepts, and (2) to demonstrate the understanding of security technology and devices, acquired by hands-on experience on security threats to computers and networks, and measures of security defense. Networking, offensive and defensive security, the three complementary parts of the course, are divided into multiple modules, covering a varied range of topics. Each module begins with a theoretical discussion, and then delves into hands-on experiments. The objective is to show that offensive security is 'fun' and intriguing, but the rigorous and detail-oriented defensive security practices effectively address the issues discussed in offensive security.

Networking Review. As a foundation, students study number systems and the concepts of TCP/IP protocol suite. We also discuss network programming and sockets, and run sample client and server programs [4].

Exercises - Students are quickly immersed into hands-on exercises that establish the concepts. First they run experiments with traceroute to various sites listed in traceroute.org [23], including a site in Switzerland and a site in Japan, analyzing paths taken to opposite sides of the world, demonstrating the concepts of routing and packet switching. They then experiment with a web communication by capturing and analyzing the underlying packet transmissions using Wireshark, a real-time tool that demonstrates the protocol layers.

```
# This script scans the IP addresses 10.2.41.50 thru
10.2.41.60, computers in this room, and see who
responds
#!/bin/bash
for ip in $(seq 50 60);
do
ping -c 1 10.2.41.$ip|grep "bytes from "|cut -d" " -f4;
done
```

Script 1. Linux bash script for "ping-sweep"

```
REM The for loop repeats for 10 times. %%A is the
variable that starts at 1 and ends at 10.
REM start command in DOS opens a new window
REM In each of these 10 windows we are sending 1000
pings of packet length 65500 each to 10.2.41.28 (DoS
victim)
REM 65500 is way beyond Ethernet MTU of 1500, and will
cause major IP fragmentation as well
@ECHO on
FOR /L %%A IN (1,1,10) DO (
        start ping -n 1000 -l 65500 10.2.41.28
)
```

Script 2. DOS script used in Classroom DDoS attack

Students also experiment with configurations of real switches and routers, available at the network/security lab, to understand the roles of each device in its designated protocol layer.

Linux Background. Students are introduced to Linux using Ubuntu, a virtual machine on their workstations, to learn basic commands and scripting language.

Exercises - Students create scripts in `bash`, a popular Linux shell, for "ping-sweeping", a technique used to identify IP addresses of live devices in a network by using the `ping` command, demonstrating the ease of use of a scripting language for malicious purposes. Script 1 shows a sample script.

Offensive Security (Penetration Testing). Students implement many offensive security techniques using virtual machines running on their Windows workstations. Kali Linux, a penetration testing platform consisting of numerous free but industry standard tools, is used as the 'attacker', and Ubuntu, a popular Linux distribution as the 'victim'. With this set up, students can freely play with intriguing and potentially harmful 'attacks', such as reconnaissance and scanning, to systematically gather information about the target, creation of backdoors to allow access to the victim machine, IP-spoofing to forge source IP address in order to conceal the identity of the attacker, and password cracking. Wireshark is used in Ubuntu as well as Kali Linux to look 'under the hood' regarding the impacts of these offensive techniques on a network. The virtual environment ensures that the 'hacking' activities stay safe inside a workstation and are not transmitted across network.

Exercises - Some exercises in this module involve `nmap` [16], `netcat` and `Ettercap` available on Kali Linux. Students experiment with `nmap` to scan devices in the subnet, and for OS (operating system) fingerprinting of Ubuntu and the host Windows system. Students then use `netcat` to create backdoor in the host workstation. `Ettercap` is used to create ARP poisoning and Man-In-The-Middle (MITM) attacks at the Link Layer. Students also play with `hydra`, a password cracking tool, and `crunch`, a password generator, to crack a password that is used to connect to Ubuntu using secure shell (`ssh`). Above tools provide the students a deeper understanding of various aspects of a systematic reconnaissance technique followed by real-world hackers.

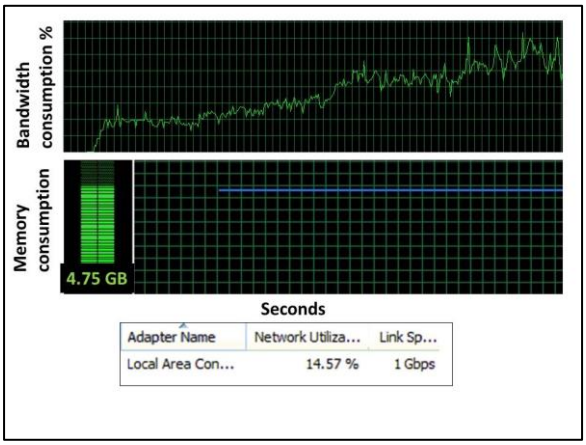

Figure 1. DDoS Attack - Network Bandwidth Degradation and Memory Consumption at 'Victim' Machine

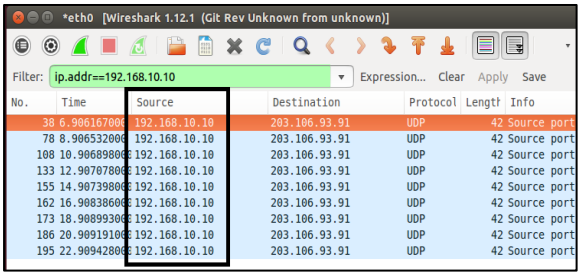

Figure 2. Wireshark Capture of Spoofed Source IP

Offensive Security (DoS). Reports show that Denial-of-Service (DoS) attacks, where an attack aims at preventing users from access to a networked resource, are becoming more and more common and powerful [18].
Exercises on Denial of Service – To begin with, students read industry reports on current Distributed DoS (DDoS) trends. Students also examine visual attack tracker tool websites, such as Attack maps by NorseCorp [17] that shows current real-time DoS attacks across the globe, and Digital Attack Map by Arbor Networks [2], which shows daily maps of global DoS attacks over past few years. Students then create a DDoS attack inside the classroom, where a seemingly simple MS-DOS script (Script 2) is run on each student machine that opens multiple DOS windows and send thousands of unusually large ping packets to the instructor's machine ('victim'). This results in rapid performance degradation at the victim in terms of bandwidth consumption and memory usage. In a sample run of two minutes, we see 14% bandwidth utilization of a 1 Gbps connection, and 4.75 GB memory consumption at the victim machine when attacked by merely six other workstations (Figure 1). This effectively demonstrates how easy it is to create a potent DDoS attack, and the reality of such attacks described in the reports and tracker websites.

Exercises on IP Spoofing – Reports show that nearly all DoS attacks are conducted using spoofed or forged IP addresses. To understand the process, students compile and run socket programs that implement IP spoofing using raw sockets. Following is an example of such a program:

```
./rawudp 192.168.10.10 21 203.106.93.91 8080
```

where UDP packets are sent using 192.168.10.10 as the spoofed or bogus source IP address. Students filter Wireshark output to verify the spoofed source IP address (Figure 2).

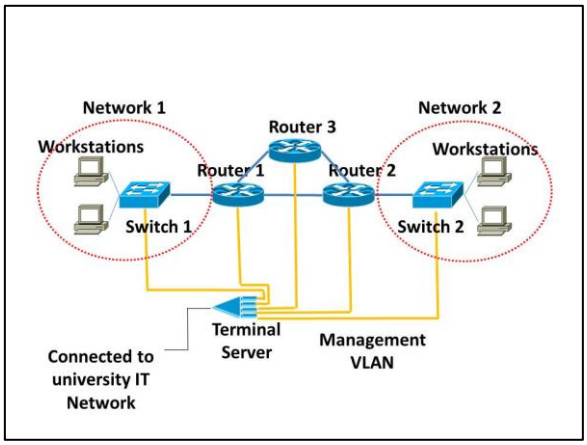

Figure 3: Network/Security Lab Configuration

Offensive Security (Application Breaches). We discuss application and web vulnerabilities in this module. In the real world, web security issues, such as SQL Injection and Cross Site Scripting (XSS), are widespread and rampant. SQL Injection is a potent web hacking technique to extract sensitive data from corporate databases. It has been used in numerous high profile hacking incidences around the globe over recent years, such as Sony PlayStation data breach [12]. XSS attacks are yet another type of injection, where malicious scripts are injected in trusted websites, and can exploit web applications to propagate malware. Equifax data breach [15] is an example of a recent significant incident where XSS has been used.

Exercises – In this module we experiment with SQL Injection and XSS techniques. As a quick introduction to databases, students first install MySQL database on Ubuntu, and learn basic SQL language. DVWA (Damn Vulnerable Web Application) [6], a web-based platform that demonstrates various web security issues, is used to create SQL Injections that expose sensitive information from the DVWA database. In another set, students experiment with various kinds of XSS scripts using DVWA. DVWA is made available to the students from this classroom alone, so that its vulnerabilities and security risks are contained only inside the classroom.

Defensive Security (Link and Network Layers). Changing topics to defensive security, a network, consisting of two switches and three router/firewalls (Figure 3), is used for the students to work with real network and security devices.

Exercises - Students learn how Link Layer attacks are prevented by configuring switch port security. For example, it is demonstrated how proper switch port security can thwart ARP poisoning attacks conducted earlier. Similar hands-on exercises with firewalls demonstrate how categories of Denial-of-Service attacks can be prevented and managed with proper configuration of these devices. Firewalls, configured correctly, can address Distributed Denial-of-Service attack and IP-spoofing experienced in the earlier modules. These experiments exemplify the efficiency of the preventative measures to address the threats discussed in the offensive security modules.

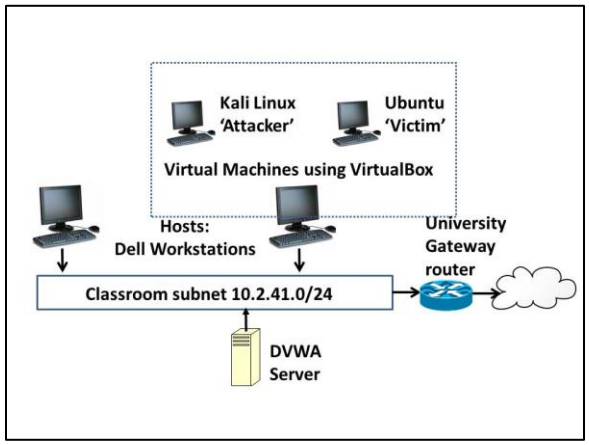

Figure 4: Classroom Configuration

Defensive Security (Transport and Application Layers). In this module we discuss cryptography and cryptographic systems that work behind every secure communication, such as secure http (https://), and Virtual Private Networks (VPNs). The role of cryptographic standards in preventing Man-in-The-Middle (MITM) attacks is discussed.

Exercises – Students work on public-private key cryptographic algorithms, such as RSA and Diffie-Hellman that are the foundation of cryptographic systems. Students conduct Wireshark experiments with https:// transactions that demonstrate SSL/TLS (Secure Socket Layer/Transport Layer Security) behind the scene, and secure shell (ssh) that demonstrate Diffie-Hellman algorithm at work.

3.3 Lab Environment

Classroom Subnet. The classroom is a subnet 10.2.41.0/24 of the university internal network that is a Network Address Translation (NAT) enabled 10.0.0.0 private address space. The IT department has given us permission to run offensive security experiments described above freely within this subnet, including scanning and DoS. In addition, DVWA is available on the browsers only in this classroom (Figure 4).

Virtual Environment. The host machines in the classroom are Dell machines with quad cores @ 3.50 GHz, 16 GB RAM and 300 GB hard drive. The virtual environment is created by running Oracle VirtualBox[25] 4.3.28. Each virtual machine is given 2 GB RAM and 10 GB virtual/5 GB real hard disk. Both Ubuntu and Kali Linux run in 64 bits in bridged adapter mode in order to get IP addresses from the class subnet.

Network/Security Lab. A Network/Security lab, developed with support from an internal grant worth $11,000 from our university, emulates a small network, where two switched networks are connected to each other by routers that act as firewalls as well (Figure 3). A number of workstations belong to these networks. A terminal server enables students to log on locally inside the university network. Students use these devices for hands-on exercises for the networking and the defensive security modules. Following is a list of lab devices.

- Cisco routers/firewalls: 3 Integrated Services 1921 Routers.
- Cisco switches: 2 Catalyst 2960 Access switches.
- Workstations: 4 Dell Optiplex 7010 MiniTower desktops.
-Terminal Server: Digi 8-Port TS MEI RJ-45 Terminal Server.

4. LESSONS LEARNED

4.1 What Worked

The following are our reflections regarding what worked. It is a combination of (1) the lesson modules and exercises, (2) hardware and software installed on the classroom workstations and in the network/security lab, and (3) the classroom subnet configuration.

Virtual Environment. The virtual environment of Kali and Ubuntu installed on each lab workstation effectively creates a vulnerable 'playground' environment. Students can freely experiment with penetration testing tools such as scanning, backdoor creation and password cracking, but nobody is hurt.

Dedicated classroom subnet. A dedicated classroom subnet, created by the university IT team is crucial in demonstrating the Denial-of-Service attack successfully. The attack packets stay confined within the classroom, and do not affect the rest of the university network.

Internet connection to the lab. This is necessary for quick and effective understanding of TCP/IP protocol layers and web security in real web transactions. Packets are sent to various parts of the world using traceroute, and paths are analyzed. Packets are captured in an unsecure web transaction to show protocol layers, and in a secure web transaction to demonstrate SSL/TLS protocol in action.

Appropriate integration of tools. Proper integration of tools is necessary to demonstrate many concepts. For example, in the Application Breaches module described in section 3.2, Ubuntu is used for a quick introduction to database, MySQL and SQL. DVWA is then used as an effective platform for SQL injection and XSS.

Network/Security Lab. A lab with real devices of switches and router/firewalls, accessible and configurable by students, provides invaluable hands-on feel of checking and configuring real devices.

4.2 Student Feedback

Undergraduate Course. The undergraduate course has been taught in Fall over last four years. We collect student evaluation in the following manner.

Our university uses Student Rating of Instruction from IDEA [9], an external course evaluation system. Our IDEA evaluations use forty questions, divided into categories regarding the instructor, the course and overall summary that the students fill online. The objectives that are chosen for this course as essential or important are:

(1) Gaining a basic understanding of the subject (e.g., factual knowledge, methods, principles, generalizations, theories),
(2) Learning to apply course material (to improve thinking, problem solving, and decisions),
(3) Developing specific skills, competencies, and points of view needed by professionals in the field most closely related to this course, and
(4) Learning how to find, evaluate, and use resources to explore a topic in depth.

Some questions on teaching methods from IDEA that have received high ratings were as follows:

Teaching Essentials:

- Demonstrated the importance and significance of the subject matter.
- Made it clear how each topic fit into the course.

Table 1. Undergraduate Classes - IDEA Scores

Term	% of students responded	Progress on Relevant Objectives (out of 5)	Ratings of Summative Questions (out of 5)	Summary Evaluation (out of 5)
Fall 2017	79%	4.0	4.4	4.2
Fall 2016	81%	4.0	4.2	4.0
Fall 2015	80%	4.5	4.4	4.5
Fall 2014	76%	4.2	4.6	4.4

Reflective and Integrative Learning:
- Encouraged students to reflect on and evaluate what they have learned.
- Related course material to real life situations.

Active Learning:
- Encouraged students to use multiple resources (e.g., Internet, library holdings, outside experts) to improve understanding.
- Involved students in hands--on projects such as research, case studies, or real life activities.

Table 1 shows the scores obtained by the course over last four years. The scores under Progress on Relevant Objectives show that the mentioned objectives were met or exceeded. Ratings of summative questions provide an average of excellent teacher and excellent course. Overall, the scores above 4.0 are marked as excellent by IDEA standards.

Workshop. The workshop was held twice each summer over past two years. It was initially designed for three days in 2017. Some participants commented in their evaluations that they would have preferred the course to run longer. Hence the course was expanded to five days in 2018.

Three-day Workshops (2017). The participants, 12 in the first workshop, 13 in the second, were given an evaluation sheet with questions at the end of the course, which they ranked using a 5-point Likert scale based on their overall course experience. The 2nd column in Table 2 shows scores per evaluation question, averaged over all participants at the two workshops in 2017. Clearly, the course worked well for the participants. Some of the participants' comments were as follows:
- 'Great info in just 3 days! Very well spent time. Awesome examples and practice.'
- 'Awesome course and instructor! Very impressed'.

Five-day Workshops (2018). The participants, 10 in the first workshop, 9 in the second, were given a similar evaluation sheet at the end of the course. In addition, they were asked pre- and post- questionnaires regarding their prior familiarity with various topics that would be covered in the course. They were given names of twelve networking and security-related topics, such as TCP/IP Protocol Stack, Switch Security and RSA encryption, and were asked of their degree of familiarity: (i) never heard of it, (ii) heard of it, but unfamiliar, (iii) somewhat familiar, (iv) familiar, or (v) highly familiar.

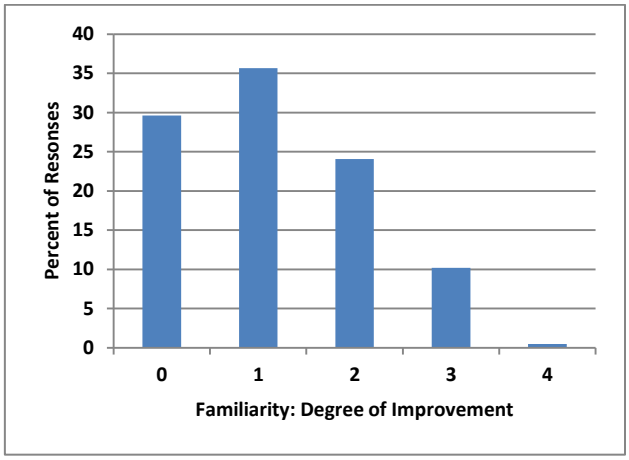

Figure 5: Five-day Workshops (2018): Familiarity of Topics in Pre- and Post- Questionnaires

Table 2. 2017 and 2018 Workshops - Evaluation scores

Question	Average Score (out of 5) 2017	Average Score (out of 5) 2018
Q1. The amount of material covered was adequate	4.7	4.8
Q2. The material was relevant	4.7	4.8
Q3. The hands-on exercises were useful	4.8	4.9
Q4. The instructor did a good job of presenting the material	4.8	4.8
Q5. The instructor addressed audience questions well	4.9	4.9
Q6. The instructor provided good hands-on assistance	4.8	4.9
Q7. Overall Satisfaction	4.8	4.8

Figure 5 shows degree of improvement in familiarity calculated from the pre- and post- questionnaire results of both workshops in 2018. 70% of the responses showed improvement in familiarity by at least one level. Out of this, 36% of the responses showed improvement by one level, and 24% showed improvement by two levels.

In addition, the 3rd column in Table 2 shows scores per evaluation question, averaged over all participants at the two workshops in 2018. Scores for questions 1, 2, 3 and 6 show improvement over the scores obtained in 2017. It appears from the participants' comments that spreading the course into five days improved the quality of the course. Some of the comments were as follows:
- 'I have seen a lot of this information in other places, but this was a fantastic comprehensive look at cybersecurity.'
- 'Lots of material, but good pacing for 5 days. Good information for both inexperienced and experienced students.'

4.3 Room for Improvement

Classroom Bound. This course, despite its success, is classroom-bound. We have to depend on the availability of this particular classroom in order to teach the undergraduate course as well as the workshop. All students and the instructor need to be physically present in the classroom in order to conduct the

experiments. Our biggest challenge right now is finding a way to extend this lab as a virtual lab and create an online class with similar objectives. We are looking into VMWare vSphere [26] products and systems in order to convert this lab into a virtual lab that students will be able to access from remote.

Offensive vs. Defensive. Another issue faced is of pedagogical nature. Compared to offensive security 'playground' that is intriguing and fun, defensive security seems harder and less appealing to students. The access to the real devices is only possible using terminals and Command Line Interface (CLI). In comparison to the offensive security tools that are available on each workstation, the access to the real devices is somewhat limited. Also, compared to the offensive security tools that are mostly free, real devices are expensive and time-consuming to set up in a real network.

5. CONCLUSION AND FUTURE WORK

In this paper we have described a novel active learning pedagogical approach for a beginning networking and security course, where students are provided with virtual and real 'playgrounds' of laboratory classroom environments. Students are introduced to theoretical background of many complex concepts, followed by numerous engaging hands-on exercises that enable them learn by doing.

As a future work, we would like to explore the possibilities of creating a similar hands-on lab environment, but virtual, that the students will be able to access from remote. This will expand the scope of this class immensely, and can be offered online to a much broader range of students and participants.

6. REFERENCES

[1] 95-758 Network and Internet Security, Course Syllabus, Spring 2017, Carnegie Mellon University Heinz College. URL:**https://api.heinz.cmu.edu/media/95-758_Network_Internet_Security_Syll_S17.pdf**.

[2] Arbor Networks: Digital Attack Map – Top Daily DDoS Attacks Worldwide. URL: **http://www.digitalattackmap.com.**

[3] Boyle, Randall J., and Raymond R. Panko. **Corporate Computer Security**. Prentice Hall Press, 2014.

[4] Comer, Douglas E., and David L. Stevens. Internetworking with TCP/IP: Client-Server Programming and Applications, volume III.Prentice Hall, 1993.

[5] Dornseif, Maximillian, et al. "An Offensive Approach to Teaching Information Security:"Aachen Summer School Applied IT Security"." **Aachener Informatik Berichte 5** (2005).

[6] DVWA – Damn Vulnerable Web Application. URL: **http://www.dvwa.co.uk**/.

[7] Fall, Kevin R., and W. Richard Stevens. **TCP/IP Illustrated, volume 1: The protocols.** Addison-Wesley, 2011.

[8] Gruber, Howard E., and J. Jacques Vonèche, eds. **The Essential Piaget.** London: Routledge & Kegan Paul, 1977.

[9] IDEA Student Ratings of Instructions. URL: **http://www.ideaedu.org**

[10] Kali Linux| Penetration Testing and Ethical Hacking Linux Distribution. URL: **https://www.kali.org/.**

[11] Louthan, George, et al. "The Blunderdome: An Offensive Exercise for Building Network, Systems, and Web Security Awareness." **CSET.** 2010.

[12] Martin, Adam, "LulzSec's Sony Hack Really Was as Simple as It Claimed", The Atlantic, April, 2011. URL: https://www.theatlantic.com/technology/archive/2011/09/lulzsecs-sony-hack-really-was-simple-it-claimed/335527/

[13] Metasploit: Penetration Testing Software. URL: **https://www.metasploit.com/.**

[14] Mink, Martin, and Rainer Greifeneder. "Evaluation of the offensive approach in information security education." **IFIP International Information Security Conference.** Springer, Berlin, Heidelberg, 2010.

[15] Morgenroth, Sven, "The Equifax Breach – The Signs Were There", Netsparker, September, 2017. URL: **https://www.netsparker.com/blog/web-security/how-equifax-data-breach-hack-happened/**

[16] Nmap: the Network Mapper – Free Security Scanner. URL: **https://nmap.org/.**

[17] Norse-Corp: Real-Time Visibility into Global Cyber Attacks. URL: **http://map.norsecorp.com/#/**

[18] NSFOCUS 2016 Q3 Report on DDoS Situation and Trends.URL: https://nti.nsfocusglobal.com/threatnewscategories/2016-q3-report-on-ddos-situation-and-trends/.

[19] Offensive Security Training and Professional Services. URL: **https://www.offensive-security.com/.**

[20] Pentesting with metasploit. URL: http://www.pentesteracademy.com/course?id=10

[21] Rapid7: Accelerate Security, Vuln Management, Compliance. URL: **https://rapid7.com/.**

[22] Timchenko, Maxim, and David Starobinski. "A simple laboratory environment for real-world offensive security education." **46th ACM Technical Symposium on Computer Science Education.** ACM, 2015.

[23] Traceroute.org. URL: http://www.traceroute.org/.

[24] Ubuntu: The Leading Operating System for PCs, IoT Devices and Servers. URL:**https://www.ubuntu.com/.**

[25] VirtualBox – Oracle VM VirtualBox. URL: https://www.virtualbox.org/wiki/VirtualBox

[26] VMware vSphere. URL:https://www.vmware.com/products/vsphere.html.

[27] Wigmore, Ivy." What is Offensive Security?" November, 2012. URL: **http://whatis.techtarget.com/definition/offensive-security**.

[28] Wireshark–GoDeep. URL: https://www.wireshark.org/.

[29] Yang, T. Andrew, and Tuan Anh Nguyen. "Network security development process: a framework for teaching network security courses". **Journal of Computing Sciences in Colleges, 21 (4), April 2006,** Consortium for Computing Sciences in Colleges.