SETTING UP AND USING A CYBER SECURITY LAB FOR EDUCATION PURPOSES *

Alexandru G. Bardas and Xinming Ou
Computing and Information Sciences
Kansas State University
Manhattan, KS 66506
bardasag@ksu.edu, xou@ksu.edu

ABSTRACT

An indispensable component of cyber security education is hands-on activities carried out in a lab to enable students to understand both offense and defense aspects of the cyber space. We describe our design and implementation of this course, and a resulting student organization Cyber Defense Club (CDC), at Kansas State University. Our 1.5-year experience in teaching this course and advising the CDC activities, including taking a team to compete in the regional Cyber Defense Competition (CCDC), shows that cyber security is very attractive to students especially when they have an environment dedicated for this type of activities.

1. INTRODUCTION

Cyber security touches nearly every part of our daily lives. Moreover, economic vitality, and national security depend on a stable, safe, and resilient cyberspace [1] [2]. We rely on this vast array of networks to communicate and travel, power our homes, run our economy, and provide government services. However, cyber intrusions and attacks have increased dramatically over the last decade, exposing sensitive personal and business information, disrupting critical operations, and imposing high costs on the economy [2]. The nation has a significant shortage of cyber security professionals who can understand and effectively thwart the growing threats. As a result, education and training in cyber security has become a national priority. Students are also eager to acquire more knowledge and skills in this critical area.

These are the reasons we started the Cyber Defense Club (CDC) at Kansas State University (K-State). The goal of the Cyber Defense Club is to teach K-State students the critical knowledge and skills needed to administer and defend computer networks and systems. As part of the CDC, we are offering two hands-on experience courses. During the class meetings, CDC members discuss and demonstrate various security topics by focusing on a number of security and hacking tools. Led by the instructor, students practice using or defending against those techniques and discuss how to secure services, applications and operating systems. All CDC activities are performed in an isolated lab network, which is behind a restrictive firewall and consists of both physical and virtual infrastructures.

In this paper, we present how we set up the lab, teach the courses, and organize the CDC activities. We hope this information can prove useful for faculty and system administrators who want to set up similar educational infrastructures in their own institution, and design hands-on courses in cyber security. We also share our experience of teaching the CDC course and advising CDC activities at K-State, with both success stories and lessons learned.

2. CYBER SECURITY LAB SETUP

The primary goal of setting up our cyber security lab was to give students the possibility to understand different offensive cyber security activities, to detect ongoing attacks and also to perform defensive actions. In order to do all these activities, students need usually administrative privileges on the hosts. In the same time all these activities

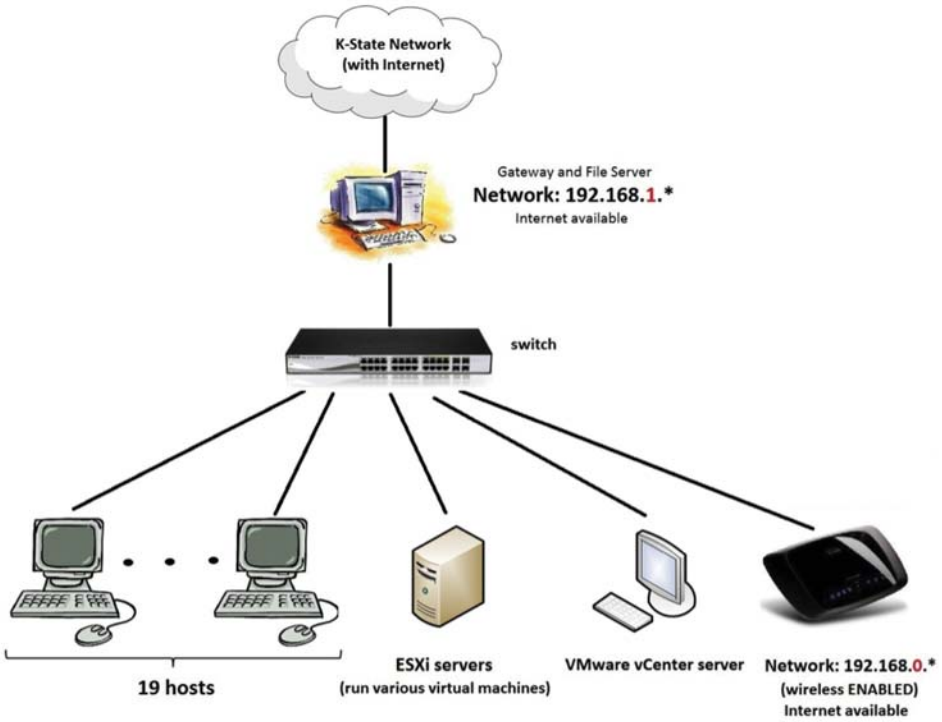

Figure 1 – CDC Lab Setup

should not disturb the rest of the campus network. Therefore we must set up an isolated network environment where students have administrative (root) privileges on the systems. *Figure 1* pictures a simplified diagram of our lab setup.

2.1 Physical Network

Our CDC network is isolated from the rest of the campus network behind a gateway. The gateway is a physical host that is connected to the campus network and to the main CDC network switch. This machine hosts the main firewall and also plays the role of a DHCP server and DNS server for the lab. Furthermore, the gateway is also a file server for our lab network (has an extra hard drive used as an NFS file-share).

Besides the gateway we have 19 hardware-identical physical hosts that are connected to our CDC main switch. Different cyber security activities require different operating systems and different tools. Hosts might get infected during the experiments. In other words, often hosts will have to be formatted and fresh images of various operating systems have to be installed. This process can be time consuming and will limit the flexibility of students and instructors. Therefore we decided to use an imaging software application (Clonezilla) to capture the host hard drive images with different operating systems and store them on the NFS file-share.

Clonezilla is an open source software disaster recovery, disk cloning and deployment solution. It enables users to clone computer's storage media (or a single partition) to a separate medium device. Data can be saved to a locally attached storage device, an SSH server, a Samba server, or an NFS file-share. Clonezilla saves and restores only used blocks in the hard disk (increases efficiency) [3]. Because the hosts are identical from the hardware perspective we were able to save "clean" images for different operating systems on the NFS file-share.

We created images for various versions of Ubuntu (*e.g.* 8; 11; 12.04), Linux Mint (*e.g.* 13), CentOS (*e.g.* 6), Backtrack (*e.g.* 5; 5R1; 5R2; 5R3), Fedora (*e.g.* 14) and Windows (*e.g.* XP, VISTA, 7). Having these images makes it very easy and fast to change the operating system on any of the physical hosts in the lab. Students are using Clonezilla to connect to the file server and "grab" a stored OS image. Usually it takes just a few minutes for a "clean" OS image to be restored on any lab machine. Furthermore, students are also able to take an image of their lab host and save their work on the file server. Later they can put that image on any of the lab machines and continue their work. As needed new operating systems can be installed on hosts, their images saved on the file server and then reused later on any of the lab hosts.

2.2 Wireless Access Point

How many devices do people connect to a network using a wireless connection? The short answer: A lot of devices. Therefore the CDC network has a wireless access point. Wi-Fi enabled devices like smartphones, laptops and/or tablets are connected to this network as needed.

2.3 Virtual Networks

The advantages of virtualization are well known: more efficient use of computer processing power, end of endless hardware purchases and upgrades, safer and faster backups and restore, *etc.* [6][7] In our CDC lab, the in-place virtualization infrastructure is very useful when recreating attack environments or when it comes to setting up different networks or scenarios.

The virtual machines and networks connected to the physical CDC network are stored on the two VMware ESXi 5.0 servers. These hosts are managed through a VMware vCenter 5 server located on a separate physical machine (see *Figure 2*). On average we have around 50 virtual machines running on the two ESXi servers. Some of these virtual machines are connected directly to the CDC networks and perform various tasks, others are behind virtual gateways interconnected using virtual switches. A significant part of the VMs directly connected to the CDC network run vulnerable services and unpatched operating systems and are used as targets in penetration testing activities. Part of the NFS partition on the gateway is accessible to the vCenter server and the ESXi hosts. This way we are able to store VMs on the network drive and also take advantage of the vSphere vMotion feature (live migration of running VMs from one ESXi host to another). The vCenter server and the rest of the virtualization infrastructure can be accessed from any CDC lab host through vSphere Client or different command-line APIs.

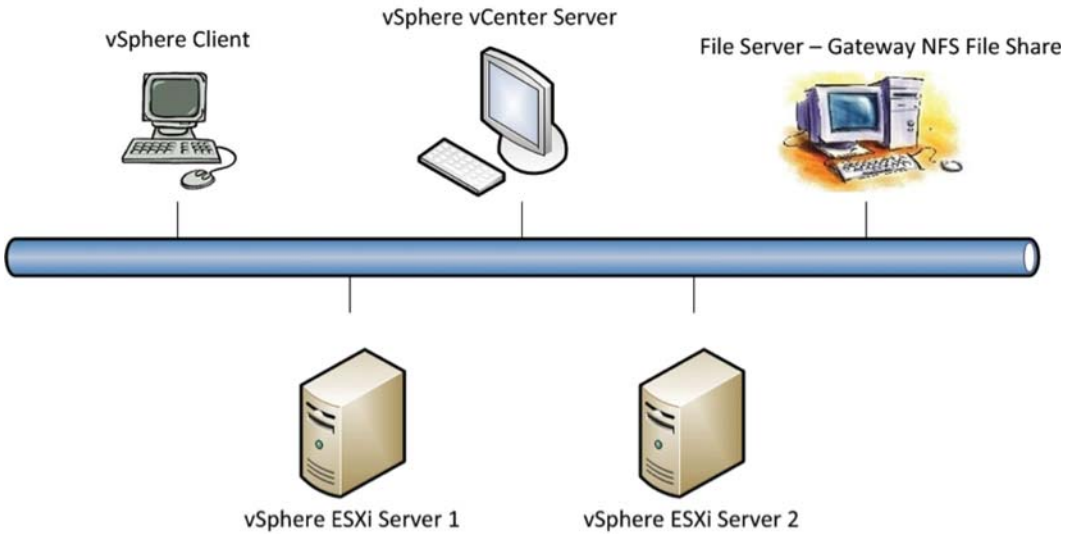

Figure 2 – CDC Virtualization Infrastructure

3. CYBER DEFENSE CLUB ACTIVITIES

The activities of the Cyber Defense Club are mainly focused on the introduction course that we are offering and on preparing a team of students for the Rocky Mountain Collegiate Cyber Defense Competition (RMCCDC).

3.1 Cyber Defense Basics Course

The course introduces students to cyber security and gives them an overview of

common offensive and defense practices. All students that want to join the Cyber Defense Club are usually taking this introductory class. Therefore the knowledge and experience level of the students varies a lot. Students attend lectures once a week and perform various hands-on activities.

Hands-on Activities and Tools

One of the course topics is "Reconnaissance." Students are being introduced to a number of information gathering practices and tools. Then they have to use the knowledge and some automated tools to scan different CDC lab machines in order to identify vulnerabilities on lab hosts. The findings include OS (*e.g.* Windows XP SP1, Metasploitable Linux, *etc.*) and services (*e.g.* vsftpd, various versions of Apache *etc.*) vulnerabilities and misconfigurations. We also installed backdoors on both physical and virtual machines (*e.g.* Energizer Battery Charger Software – Arucer Backdoor).

Usually students use Backtrack as operating system and different port scanners and vulnerability scanners (*e.g.* Nmap and Nessus). They also use service-specific vulnerability scanners when needed (*e.g.* Nikto – web server scanner). Most of the students are able to find most of the vulnerabilities and misconfigurations on the network. Other course activities include using various frameworks (*e.g.* Core Impact Pro, Metasploit) to exploit the discovered vulnerabilities on the network, monitor network traffic, exploit wireless networks or Denial-of-Service attacks. Most of the tools and frameworks that are used in the lab are open source tools. However, there are a few exceptions (*e.g.* Core Impact Pro).

Core Impact Pro is stated to be the most comprehensive software solution for assessing the real-world security of endpoint systems and email users, mobile devices, network devices and systems, web applications, and wireless networks [4]. We have obtained a free educational copy of Core Impact for use in the CDC classes. For obvious security reasons our copy of the software is customized and will run only on our private network. The license for such a product is usually in the tens-of-thousands of dollars per year. Students are usually very excited to get familiar with such a tool, since usually they do not have this opportunity outside the CDC lab.

3.2 RMCCDC and CCDC

Students that are interested in cyber security and completed the Cyber Defense Basics class are given the possibility to work on topics of their choice and prepare for the Rocky Mountain Collegiate Cyber Defense Competition (RMCCDC). The RMCCDC focuses on the operational aspects of managing and protecting an existing commercial network infrastructure. Every team will be securing, managing, and maintaining a small business network – responding to business tasks called injects, and maintaining a core group of critical services such as a mail server or an e-commerce site, while a live Red Team that is attempting to break into the teams systems [5]. The winner of the regional competition will advance to the National Collegiate Cyber Defense Competition (CCDC).

The best twelve students will be on the competition team roster (8 team members and 4 alternates). Throughout the semester, students work on configuring and securing different services on physical and virtual machines. A good example in this sense is one

of the CDC virtual practice networks (see *Figure 3*). Students have to setup and configure such a network, respond to different challenges and keep services up when network is under attack.

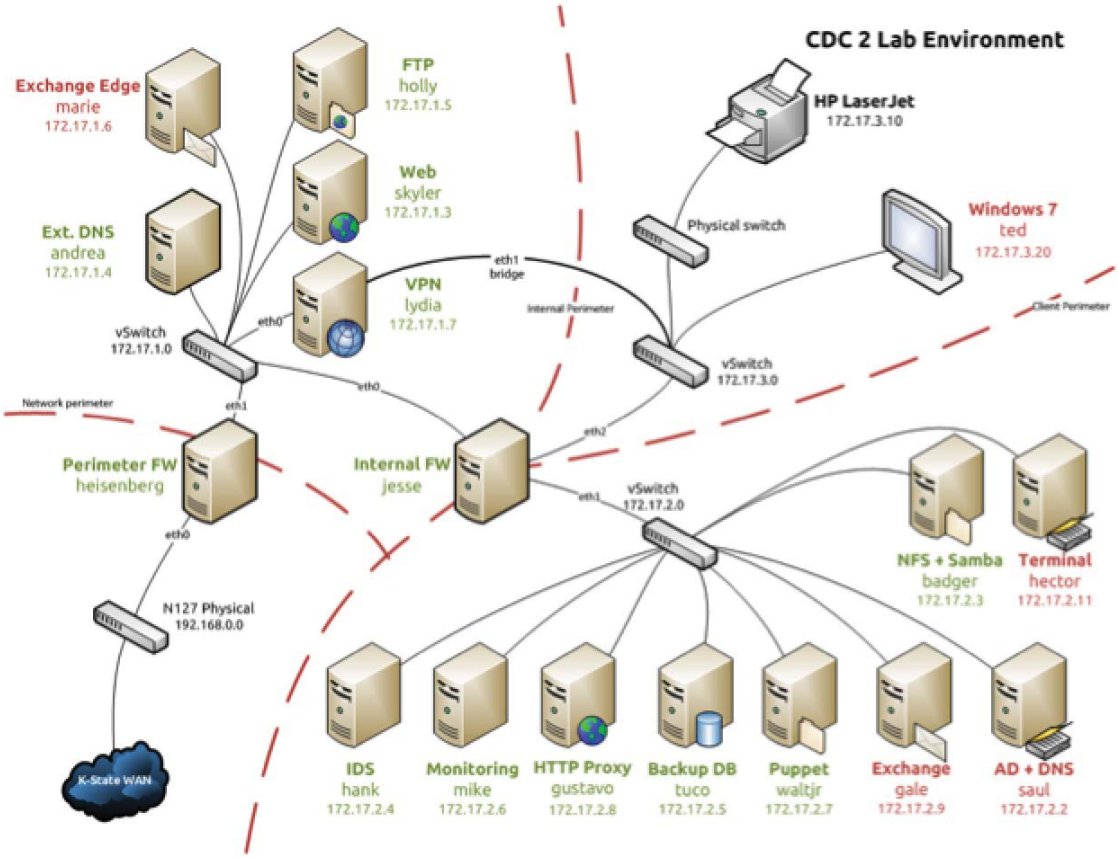

Figure 3 – CDC virtual network

4. RESULTS

We observed that students are interested in cyber security and enjoy hands-on activities. The course and teacher evaluations at the end of every semester were very good and the fact that a significant number of students are trying to make our competition team is very encouraging. The idea of having a lab where they are allowed to try offensive and defensive actions seems to be very attractive to students. A significant number of students brought their machines to the lab and performed various penetration testing actions (including running Core Impact Pro) to see if their host looks secure. Other students spend a lot of hours in the lab trying to configure different services and tools.

5. CONCLUSION

Cyber security is very attractive to students especially when they have an environment dedicated for this type of activities. The goal of the Cyber Defense Club at Kansas State University is to teach students the critical knowledge and skills needed to administer and defend computer networks and systems. This paper gave an overview of

a possible cyber security environment setup where faculty and students can perform real-world hands-on cyber security activities.

ACKNOWLEGEMENT

We would like to thank Ian Unruh and the rest of the CDC2 members for their work in the Cyber Defense Club, especially for setting up the virtual practice networks and for their wiki page contributions. The materials presented in this paper are based upon work supported by the National Science Foundation under Grant no. 1129534. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation. We would also like to thank the Department of Computing and Information Sciences at Kansas State University for supporting the CDC activities.

REFERENCES

[1] White House -National Security Council, *http://www.whitehouse.gov/cybersecurity* retrieved November 10, 2012

[2] Department of Homeland Security, Cyber Security Overview, *http://www.dhs.gov/cybersecurity-overview,* retrieved November 11th, 2012

[3] Clonezilla Web Page, *http://clonezilla.org,* retrieved August 15th, 2012

[4] Core Security, Core Impact Pro, *http://www.coresecurity.com/content/core-impact-overview,* retrieved July 28th, 2012

[5] National Collegiate Cyber Defense Competition, *http://www.nationalccdc.org,* retrieved February 2nd, 2012

[6] Bill Johonnesson, Summary of the Advantages of Virtualization, *http://ezinearticles.com/?Summary-of-the-Advantages-of-Virtualization&id=4273097*, retrieved November 15th, 2012

[7] VMware Benefits of Virtualization, *http://www.vmware.com/virtualization/,* retrieved November 15th, 2012