Platoon: A Virtual Platform for Team-oriented Cybersecurity Training and Exercises

Yanyan Li and Mengjun Xie
Department of Computer Science
University of Arkansas at Little Rock
{yxli5, mxxie}@ualr.edu

Abstract

Recent years have witnessed a flourish of hands-on cybersecurity labs and competitions. The information technology (IT) education community has recognized their significant role in boosting students' interest in security and enhancing their security knowledge and skills. Compared to the focus on individual based education materials, much less attention has been paid to the development of tools and materials suitable for team-based security practices, which, however, prevail in real-world environments. One major bottleneck is lack of suitable platforms for this type of practices in IT education community. In this paper, we propose a low-cost, team-oriented cybersecurity practice platform called Platoon. The Platoon platform allows for quickly and automatically creating one or more virtual networks that mimic real-world corporate networks using a regular computer. The virtual environment created by Platoon is suitable for both cybersecurity labs, competitions, and projects. The performance data and user feedback collected from our cyber-defense exercises indicate that Platoon is practical and useful for enhancing students' security learning outcomes.

Keywords

Virtual Platform; Cybersecurity Practices; Team-oriented Exercises

1. INTRODUCTION

Hands-on exercises and competitions are important and effective means for cybersecurity education and training. They can significantly boost students' interest in security and enhance their security knowledge and skills, which makes students more likely to be recruited and retained in cybersecurity. However, most of security education materials (e.g., security labs and projects) in academic settings are developed for individual students. Much less attention in higher education has been paid to team-based security exercises, which, however, are equally important in real world. One of the major reasons is lack of suitable platforms for this type of exercises and practices.

Virtual platforms have become popular in cybersecurity education, especially for hands-on labs and exercises [1, 8]. However, it is often difficult or expensive to implement team-based security exercises using those platforms as they primarily target individual students. Du *et al.* described SEED Labs, a suite of hands-on security labs in [7]. Students can download the preconfigured virtual machine (VM) images and instantiate them using a VM hypervisor (e.g., VirtualBox) to do the labs. The environments created by the SEED Labs and other similar labware usually contain a single VM or a simple, small network with a few VMs since they are sufficient for those labs designed to facilitate class learning. Sun *et al.* proposed a security experiment platform called V-NetLab [9], which is mainly for security research instead of education. Another similar research platform is DETER lab [3], which is a testbed designed for developing and testing new security techniques against large-scale network threats, e.g., worms and DDoS attacks. Those research platforms are not designed for team-based exercises, either. Leveraging cloud computing, cloud-based lab platforms also become popular. In [15], Xu *et al.* presented a cloud-based experiment platform, called V-Lab, which has been used for networking and security courses. However, it is not clear how easy or difficult to implement team-based exercises using V-Lab as it is not open-source. An open-source platform called open cyber challenge platform (OCCP) [12] can be used for team-based practices. However, OCCP is not mature and cannot accommodate multiple teams.

Given the complexity of cyber-attacks, effective cybersecurity training and education should not only leverage individual-oriented courseware but also incorporate team-oriented platforms, which are able to create a realistic network environment that requires a team of people with a comprehensive set of skills to manage and protect. Team-based exercises in a network environment that mimics real world business networks can not only improve individual learner's knowledge and skills but also instill the spirits and soft skills of teamwork and collaboration. Those team-based exercises accelerate students' learning process and help students to exchange ideas, quickly identify and solve problems, formulate joint defense strategies and so on. From previous studies [4, 13] and our own experiences, team-based exercise is one of the keys to motivate and retain students in cybersecurity. Recently, team-based cybersecurity competitions such as collegiate cyber defense competition (CCDC) [11] and iCTF [10] are increasingly popular. Those competitions

SIGITE'16, September 28-October 01, 2016, Boston, MA, USA

DOI: http://dx.doi.org/10.1145/2978192.2978230

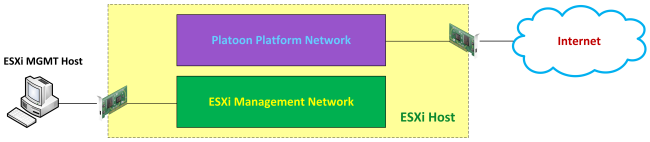


Figure 1: Overview of the Platoon platform

stimulate students' interests and aspirations in cybersecurity [2, 6, 5, 14]. Therefore, it is highly desirable to have an effective cybersecurity platform for team-based practices. However, building such a platform using the aforementioned systems is cumbersome and time-consuming since those systems are primarily used for personal exercises and often do not support team-based practice.

There exist virtual platforms suitable for team-based security exercises, e.g., the CSSIA Virtualization Center, which has been used to host virtual competitions for regional CCDCs and National Cyber League (NCL). However, such environments use commercial systems with expensive license fees and may not be able to offer access to participating instructors at their requested times. Based on our experiences, a low-cost, auto-deployable platform using a regular PC appears a most flexible and practical approach for instructors with limited resources.

In this paper, we present Platoon, a virtual **Plat**form for team-**o**rien**t**ed cybersecurity exercises. The Platoon platform allows for creating one or more virtual networks that mimic real-world corporate networks using a regular computer in a quick and automatic manner. The environment created by Platoon is suitable for both cybersecurity labs, competitions, and projects. The performance data and user feedback indicate that our proposed platform is practical and useful for enhancing students' security learning outcomes.

The rest of this paper is organized as follows: Sections 2 and 3 present the design and deployment of the Platoon platform, followed by the description of system usage in Section 4. Section 5 details the performance and user assessment of the platform, and Section 6 concludes this paper.

2. SYSTEM DESIGN

The Platoon platform is designed to be a versatile system for various security education scenarios such as assisting security courses in high schools or colleges, hosting cyber-defense competitions, and creating environments for IT training or security research. The network design of Platoon makes it particularly suitable for team-based exercises. Individuals can also use the platform to perform traditional security labs and exercises directly by applying appropriate VM images. To maximize its impact to security education, we set the following objectives for the platform:

- *Native support for teamwork.* The platform is aimed to support tasks/labs/projects for multiple teams as well as individuals, which makes Platoon distinctive from many existing educational systems that are primarily for individual based learning. The emphasis of teamwork support reflects our observation that security operations and cyber defense in real world often require strong collaboration involving multiple people with complementary expertise, which unfortunately is not well prepared using current security education platforms.
- *Cost-effectiveness.* The cost for building and maintaining the platform should be affordable for less resourceful organizations or individuals. For example, the requirement of a regular PC and free software plus a few hours labor of an undergraduate student is much more attractive and affordable than the requirement of a powerful server, commercial software and multi-day professional onsite installation.
- *Functionality.* The platform must be able to instantiate a network environment that reflects a common business network setting and includes a common set of services (e.g., web and email) to realize the security tasks that demand teamwork. For example, Platoon is expected to create networks suitable for blue teams to practice system hardening and network defense skills. In addition, the functionality should be realized with high fidelity and satisfying performance.
- *Deployability.* The platform should minimize requirements (e.g., hardware, networking) for deployment and introduce minimal change to existing network and environment configurations. Moreover, the platform should be deployed in an automatic manner with minimal human intervention.

With those objectives, we apply free version VMware ESXi hypervisor to build the Platoon platform. Figure 1 depicts its high-level design. Two isolated networks, the Platoon platform network and ESXi management network, are created in the ESXi host to separate network accesses for system management from user accesses to the virtual environment.

The Platoon's internal structure is depicted in Figure 2, which is framed in a scenario of cyber-defence competition or exercise. The blue team networks in the figure refer to the virtual networks to which security hardening and cyber-defense operations are applied. The Platoon platform can create a full-blown security competition/training environment that supports simultaneous accesses from multiple blue teams, the red team, and other supporting teams.

A blue team is a group of students or trainees who are required to protect the assigned virtual network and servers and to defend against the attacks launched by the red team. A red team is constituted by professional penetration testers whose goal is to assess the security of a blue team network by compromising their servers or disrupting their services. A white team consists of room monitors or onsite judges, whose duties include enforcing policy compliance, assisting task dispatch, and reporting technical or logistical issues. A gold team is comprised of representatives from industry and academia as well as competition organizer, whose jobs are to assist or manage the competition/training. Platoon allows for creating all those teams and assigning them appropriate accesses to the virtual environment created by the platform. When Platoon is used in teaching as an academic lab environment, students can be grouped into one or more blue teams for doing their assignments. Some teams such as red and white teams may not be needed in this case.

Platoon consists of five main components: blue team server network, edge router, central virtual switch (vSwitch), scoring engine, and perimeter firewall. The platform, i.e., the block with green dotted lines in Figure 2, is provisioned by a bare-metal hypervisor (VMware vSphere ESXi). We have developed installation scripts to automate platform deployment on a physical computer. Platoon can also be deployed on a VM instead of bare-metal. However, the bare-metal deployment provides much better performance and is also much easier (e.g., the Ubuntu system needs customization

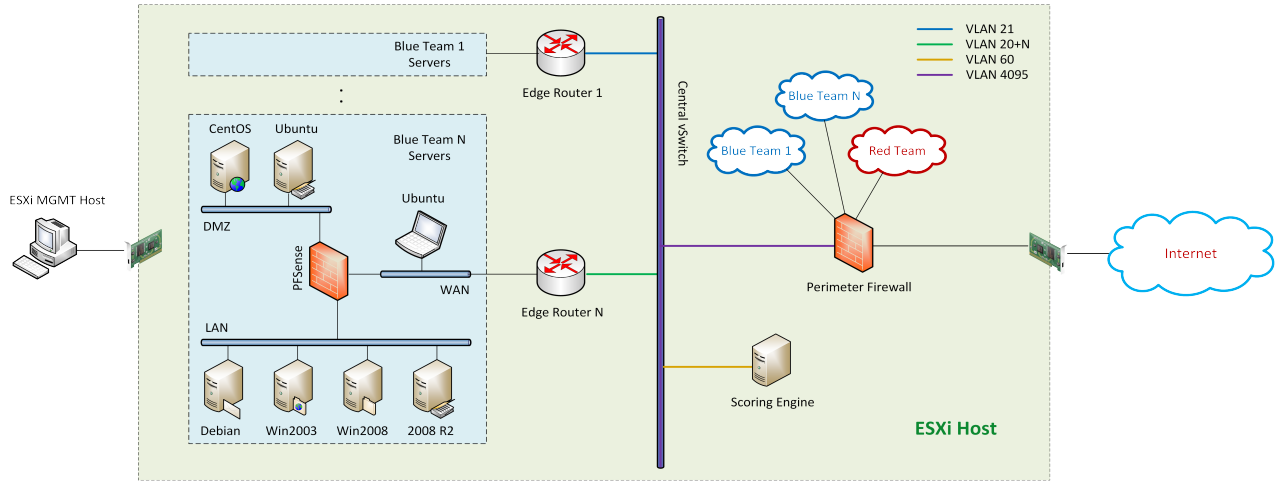


Figure 2: Network topology of the Platoon platform

Table 1: Sample services maintained by a blue team

Server	Hosted Services
CentOS Server	Web (HTTP and HTTPS)
Ubuntu Server	DNS
Debian Server	POP3
Windows 2003	FTP
Windows 2008	Distributed File System (DFS)
Windows 2008 R2	Active Directory, DNS

of KVM for VMware ESXi to function properly). Therefore, we use bare-metal deployment in our implementation.

Platoon Blue Team Server Network is a virtual server network that blue teams are required to maintain and protect. The network topology and hosted servers are based on the network setting used in recent regional collegiate cyber-defense competitions. A Platoon blue team network provides a small business network setting with common application servers on the DMZ (Demilitarized Zone) and LAN segments. Moreover, a workstation is provisioned on the "WAN" (Wide Area Network) segment to provide client access from the "Internet." The firewall is configured to separate DMZ and LAN from WAN. Table 1 lists a set of sample servers and services provisioned for a blue team, which can be easily changed and updated. By offering such a business network to blue teams, Platoon users can obtain team-based cybersecurity skills and experiences that can be directly applied to real-world working environments.

Platoon Edge Router is a virtual router (current implementation using OpenWRT) that connects to a blue team server network and acts as that network's gateway router. It also provides one-to-one NAT (network address translation), advanced QoS (quality of service) and so on. We leverage the one-to-one NAT function to map a "public" IP address to the IP address for each virtual server. By doing so those virtual servers can be accessed from outside with different destination IP addresses instead of using the same IP address but different port numbers (i.e., port forwarding), which aims to enhance the fidelity of the virtual environment to a real-world network environment.

Platoon Central vSwitch is a built-in virtual switch provided by VMware vSphere ESXi that functions much similar to a physical switch and is responsible for VLAN (virtual LAN) creation and management. The VLAN is used to separate different networks, e.g., blue team server networks and scoring engine network. The central vSwitch assigns a distinct VLAN ID to each subnet to isolate the communications for different subnets. As shown in Figure 2, VLAN 21, ..., 20+N and 60 are created for blue team 1 to N (the number of total blue teams) server networks and scoring engine network, respectively. The link between the central vSwitch and the perimeter firewall is a VLAN trunk link that carries traffic for all VLANs including VLAN 21, ..., 20+N and 60.

Platoon Scoring Engine offers real-time service scores for each blue team by probing the status of each required service maintained by the blue team. The tested services are decided by the instructor or organizer and they usually include common services such as HTTP/HTTPS, DNS, SMTP, POP3, and particular services to be tested. Each blue team is assigned a unique ID so that different teams can be distinguished at the scoring board. The scoring engine is given a public IP address so that blue teams can check their service status in real time during an exercise or competition.

Platoon Perimeter Firewall controls the communications between the platform and the Internet, prevents malicious traffic leaving out of the platform, and meanwhile protects the platform from being attacked from outside. The perimeter firewall is a VM running pfSense, which is an open-source customized distribution of FreeBSD and provides powerful and flexible firewall and routing functions. The perimeter firewall also manages VLAN subnets and is the key to achieve the inter-VLAN communications. Moreover, OpenVPN servers are set up on the perimeter firewall to provide authenticated, secure access for remote teams. The three small clouds illustrated in Figure 2, which are directly connected to the perimeter firewall, are VPN tunnel networks for Blue Teams 1 and N and Red Team, respectively. These VPN tunnel networks are managed by the corresponding OpenVPN servers.

3. DEPLOYMENT

To achieve deployability, we have developed a set of code scripts by which we can deploy Platoon on a computer in an easy and automatic manner. Figures 3 and 4 present code

```
# Create vSwitch1
esxcli network vswitch standard add --vswitch-name vSwitch1
esxcli network vswitch standard portgroup add --portgroup-name
"Internet" --vswitch-name vSwitch1

# Create vSwitch2 with VLANs
esxcli network vswitch standard add --vswitch-name vSwitch2
esxcli network vswitch standard portgroup add --portgroup-name "vLAN21"
--vswitch-name vSwitch2
esxcli network vswitch standard portgroup set --portgroup-name "vLAN21"
--vlan-id 21
esxcli network vswitch standard portgroup add --portgroup-name "vLANs"
--vswitch-name vSwitch2
esxcli network vswitch standard portgroup set --portgroup-name "vLANs"
--vlan-id 4095

# Create vSwitch3
esxcli network vswitch standard add --vswitch-name vSwitch3
esxcli network vswitch standard portgroup add --portgroup-name "B1_WAN"
--vswitch-name vSwitch3
```

Figure 3: Code snippet for creating virtual subnets

snippets for creating virtual subnets and deploying virtual machines. Compared to other virtual platforms that only provide remote access interface, Platoon not only offers similar remote access mechanisms (e.g., RDP or SSH) but also makes it possible for security learners to build and fully control a security practice environment on their own hardware, which helps improve learners' understanding and skills on system and network management.

Platoon can run well on consumer grade off-the-shelf hardware. We deployed and tested Platoon on a Dell OptiPlex 990 desktop PC, which is 5 years old with an Intel i7-2600 CPU, 16GB memory and two 1TB HDD hard drives. The deployed system was tested by hosting cyber-defense exercises with two blue teams (5 students each) and a red team and it achieved satisfying performance. We also deployed Platoon on a Dell R410 server (12 cores and 48 GB memory) to host a cyber-defense competition. The platform worked very well in the 6-hour competition with 6 blue teams (up to 8 persons in one team) and 1 red team. Over 40 undergraduate and graduate students from 7 universities participated in the competition.

In deployment, the ESXi hypervisor has to be installed first. To isolate ESXi management network from Platoon platform network and realize remote VM management, two physical network cards (NICs) each associated with a unique IP address are required on the Platoon machine. Through the IP address assigned for ESXi management, the Platoon administrator (e.g., class instructor or competition organizer) can use the vSphere Client to easily and remotely perform various VM operations such as creating VM snapshots, applying snapshot-based recovery and monitoring platform performance.

Then the installation scripts are applied to download and instantiate VM images and perform network and system configurations. The number of blue teams to be created, e.g., 4, can be configured during installation. However, the actual number of blue team networks is constrained by the hardware resources on the deployment computer. The installation scripts will first check whether the hardware meets the minimal resource requirements, e.g., at least 8GB memory for one blue team. If the minimal requirements are not met, an error alert will be displayed and the installation will abort. Otherwise, all necessary preconfigured VM images will be downloaded from the default or specified website and instantiated. Preconfigured VM images are provided for routers, firewalls, blue team servers, scoring engine and

```
# Create CentOS VM directory and change into it
mkdir -p ${DATASTORE_PATH}/${VM_FILENAME}
cd ${DATASTORE_PATH}/${VM_FILENAME}

# Download CentOS
wget ${CENTOS_DOWNLOAD_URL}

# Convert VMDK from sparse to Thin
vmkfstools -i centos.vmdk ${VM_FILENAME}.vmdk -d thin

# Update CentOS VMX file content
sed -i "s/centos.vmdk/${VM_FILENAME}.vmdk/g" centos.vmx
echo "ethernet0.networkName = \"${VM_NETWORK}\"" >> centos.vmx

# Register CentOS VM which returns CentOS ID
CENTOS_ID=$(vim-cmd solo/register ${DATASTORE_PATH}/${VM_FILENAME}/
${VM_FILENAME}.vmx)

# PowerOn CentOS VM
vim-cmd vmsvc/power.on ${CENTOS_ID}
```

Figure 4: Code snippet for deploying virtual machines

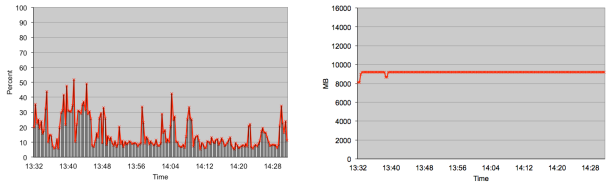
workstations in different application scenarios. For example, we have created a Ubuntu server image with a variety of misconfigurations which can be used in various scenarios, e.g., a vulnerability scanning lab or a cyber-defense competition. The OpenWRT router and perimeter firewall are configured to realize layer-three networking functions, e.g., partitioning the virtual network into multiple subnets such as VPN tunnel network, blue team server network, and scoring engine network. A pfSense firewall inside a blue team server network is employed to further divide that subnet into three segements, i.e., LAN, DMZ, and WAN. The virtual servers on each of these three segements are communicated with one another via the ESXi vSwitch.

4. USAGE

Platoon requires VPN (currently using OpenVPN) for end users (e.g., students or trainees) to access the virtual environment. The use of VPN brings multiple benefits: 1) The platform only requires one public IP address and is still able to create complex networks for the virtual environment; 2) User authentication is strengthened with public key cryptography; and 3) All network traffic between end users and the platform is encrypted.

The platform administrator usually is responsible to create user accounts on the OpenVPN server sitting on the perimeter firewall and distribute OpenVPN account credentials to the platform users. With OpenVPN credential files (i.e., .ovpn and .key files), an end user can use an appropriate OpenVPN client (e.g., Tunnelblick on Mac and OpenVPN client on Windows) to access the virtual network environment created by Platoon. As the first step, a user establishes a VPN connection to the OpenVPN server and obtains an IP address from the VPN tunnel network. Multiple VPN tunnel networks are created to accommodate multiple teams, whose access privileges are strictly regulated, that is, a user is only able to access certain network and servers based on his or her assigned team and role. For example, a blue team member is allowed to access his or her blue team network but not other blue team networks; A red team member is allowed to access all blue team networks. In addition, servers in different blue team networks are not allowed to communicate with each other. The purpose of the restricted setting is to isolate each blue team's management domain and to avoid network interferences among blue teams.

Once users are connected to Platoon via an OpenVPN connection, they can conduct network or server management



(a) CPU usage (b) Memory usage

Figure 5: CPU and Memory usage on the ESXi host

operations in the same way as they do on a real-world network or server. For example, blue team members can access a Linux or Windows server in their assigned blue team network through common access mechanisms such as SSH or RDP as usual. As the pfSense configuration interface is Web based, to set up the pfSense firewall inside a blue team network, a blue team member needs to launch a Web browser from the workstation on the WAN segment to connect to the pfSense.

5. EVALUATION

We have deployed Platoon on a Dell OptiPlex 990 PC for small cyber-defense exercises with 2 blue team networks and on a Dell R410 server for hosting a competition with 6 blue teams networks. Considering that security instructors or learners may only have a low-budget PC (e.g., our old Dell PC) at their disposal, the performance of Platoon on a PC is more important for security teaching or practice in a less resourceful setting. Therefore, we report the system performance on the old Dell PC in this section. We also present students' feedback on the cyber-defense exercise when it was applied in and out of class teaching.

5.1 System Performance

The performance measures were collected during an extracurricular cyber-defense exercise conducted in 2015. The exercise involved 10 computer science undergraduate students (4 females and 6 males, ranging from sophomore to senior) interested in security. None of those students had cyber-defense experience and most of them could be classified as security novice prior to the exercise. They formed 2 blue teams with 5 students in each team. In addition, 3 undergraduate and 1 graduate students who had security skills and experiences formed the red team and launched various attacks to both blue teams during the 4-hour exercise.

Compared to the setting shown in Figure 2, Windows Server 2008 and Windows Server 2008 R2 were removed from the blue team server network to reduce students' duty given that each team had only 5 members. A team packet including the exercise policy, the blue team server network topology along with the network configurations was provided to all the participants 3 days prior to exercise. Both team started with the identical configuration including 4 servers, 1 workstation and 1 pfSense firewall. Five services including HTTP, HTTPS, DNS, POP3 and FTP were required to maintain and secure but only HTTP and FTP services were up and running at the beginning. Therefore, besides hardening the network and servers, the blue teams also needed to configure and run the rest 3 services and protect them from being compromised.

We collected CPU usage, memory consumption, network traffic and disk read and write rates during the exercise. As the network traffic and disk read and write rates are pretty low most of the time, we only report CPU and memory usage data here. Figure 5 depicts the resource consumption of the ESXi host at the beginning of the exercise, which is the most active period for blue teams as they usually perform most extensive system hardening, updates, software downloading and configurations at the beginning. From Figure 5a, we can see the CPU load of the platform stays low (less than 20% on average) for most of the time. The overall CPU load spikes from time to time due to system updates and software installation but all of those spikes are brief.

In general Windows servers were given 1-2 GB memory and Linux servers were given 512MB to 1GB memory. Figure 5b presents the overall granted memory of the 16 VMs in the exercise. Typically, the amount of granted memory reflects the need of VMs on physical memory but not the actual memory consumption due to memory sharing managed by hypervisor. Therefore, the memory actually consumed is usually much smaller than the granted memory. From Figure 5b, we can see that the total granted memory is around 9GB. We can also observe that the curve dips a little at around 13:38. That is because one blue team requested to restore one server to its initial state After the restoration completed, the memory curve goes back to flat.

We also used the same hardware to run another exercise in spring 2016 with 2 blue team networks. However, two Windows servers were added back to the blue team network this time. We observed a minor increase of CPU load and more memory being granted. In both exercises, students reported smooth user experience in managing servers and networks.

5.2 User Feedback

We evaluated the effectiveness of Platoon and the exercise through pre- and post-surveys. The first survey was given out 3 days prior to the exercise to gain the baseline of students' knowledge, skills, and experience in cyber defense. The second survey was given immediately after the exercise. All 10 students responded to the first survey and 8 of them responded to the second one.

The same 8 questions were asked in the both surveys. The first 3 questions are on system management; the questions 4-7 are relevant to cyber defense skills; and the last question is about the opinion on teamwork in cybersecurity operations. Likert scale (no experience to very experienced, or strongly disagree to strongly agree) is used for all questions. The average scores of each question in both surveys are presented in Figure 6. By comparing the scores, we can clearly see that students' skills in both cyber defense and system management have improved in various degrees. The most significant improvement in server management is on Linux management, which may be attributed to that more students (3 out of 4 on servers) worked on Linux servers. Overall, the most significant improvement lies in network security skills. As our red team was not aggressive enough to immediately down the server after break-in, time was given to the blue team under attack to detect red team's intrusion and behavior and to create firewall rules to block further intrusion. Evidently, more recognition on the importance of teamwork was gained by the students as the exercise convincingly demonstrated that cybersecurity enforcement needs effective teamwork and collaboration.

Q1. Rate your experience in Windows server management
Q2. Rate your experience in Linux server management
Q3. Rate your experience in network management

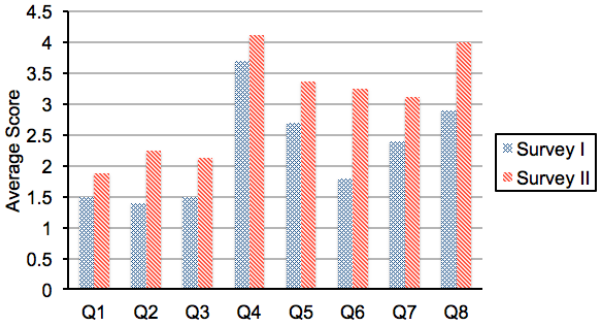


Figure 6: Survey Results. Scale from 1 to 5. 1 means no experience or strongly disagree. Survey I is pre-survey and Survey II is post-survey.

Q4. You have a strong motivation to learn and apply cyber defense
Q5. Rate your knowledge/skills in hardening servers
Q6. Rate your knowledge/skills in securing network
Q7. Rate your knowledge/skills in identifying attacks
Q8. Teamwork is a critical element for effective cyber defense

We also conducted a Platoon based cyber-defense exercise as a component of college Computer Security course (senior level class) in 2016. After the testing run in 2015, we offered a cyber-defense exercise as an optional assignment to the students taking the class in spring 2016. Different from the 2015 exercise which gave students little preparation, we scheduled the 2016 exercise in the later part of the semester assuming that interested students would have reasonable security background at that time. We also offered 3 whole-day practice sessions each in a different day in the 2 weeks prior to the 2016 exercise. Eight students (2 blue teams with 4 students in each) participated in the 5-hour exercise in one Saturday afternoon in April.

To have a deep understanding of the platform and exercise, we asked the participating students to provide their opinions and comments voluntarily. The general feedback from the students is positive and encouraging. Some excerpts from their comments are as follows:

- *The competition itself was more exciting and interesting than I had expected. I definitely enjoyed the whole experience.*
- *During the competition I learned that it was not enough to know the principles of how the different services work. It was necessary to know the steps needed to set up and configure the services in the different platforms. It was also necessary to have good communication, research, and analytical skills, because some problems could be caused by missing components, or by making mistakes following the instructions, or by failing to understand the differences between the generic instructions found online and the actual name and IP address of the hosts, or simply by mistyping some configuration entry, and an extra set of eyes came in handy. I also learned that there is a lot of good information online, but one must have a discerning eye to know which information is pertinent. Finally, I learned that I know almost nothing about how to find or exploit vulnerabilities.*
- *I found the experience challenging but exciting. Not only was it thrilling, but I also gained experience I could use on the job.*
- *Even though it only lasted a few hours, this activity really brought all what was learned in class about network security together, ... I hope this activity, or a variation of it, perhaps with a dedicated red team vs. a blue team, becomes permanent part of the class.*
- *This assignment was very useful. I really liked the rooms and setting of the competition. It was very open and comfortable.*

Some common issues reflected in the students' feedback include insufficient knowledge in Linux commands and administration, no experience in firewall rules and management, not enough time for practice, no exercise on weekend etc. A major challenge presented to many students for using the system is in accessing the virtual environment through OpenVPN, which they had never experienced. We will address raised technical and logistic issues and make the exercise a regular part of the course in future.

6. CONCLUSION

In this paper, we have presented Platoon, a low-cost, team-oriented virtual platform for cybersecurity exercises. Platoon can be built using a regular PC and free software. We have developed the deployment scripts that automate the system installation and configuration. The Platoon platform can be applied both in academic curriculum for implementing hands-on labs and in extracurricular activities for hosting cyber-defense competitions. The experimental results demonstrate the efficacy of our platform with modest hardware. The survey results indicate that Platoon is able to improve users' cyber-defense skills. Given its low cost, applicability, and flexibility, the platform is expected to help fill the gap between security education and real-world demands through team-based cybersecurity practices. Platoon will be released as an open-source project on Github once we complete documentation and code cleaning.

Acknowledgments

This work was supported in part by the National Science Foundation under Award Number 1338102 and Amazon with an AWS in Education Research grant.

7. REFERENCES

[1] R. Bajcsy, T. Benzel, and et al. Cyber defense technology networking and evaluation. *Commun. ACM*, 47(3):58–61, March 2004.
[2] Y. Bei, R. Kesterson, K. Gwinnup, and C. Taylor. Cyber defense competition: A tale of two teams. *J. Comput. Sci. Coll.*, 27(1):171–177, October 2011.
[3] Terry Benzel. The science of cyber security experimentation: The deter project. In *Proc. 27th ACSAC*, pages 137–148, 2011.
[4] R. Cheung, J. Cohen, H. Lo, and F. Elia. Challenge based learning in cybersecurity education. In *Proc. Intl. Conf. on Security & Management*, volume 1, 2011.
[5] Art Conklin. The use of a collegiate cyber defense competition in information security education. In *Proc. 2nd InfoSecCD*, pages 16–18, 2005.
[6] G. Conti, T. Babbitt, and J. Nelson. Hacking competitions and their untapped potential for security education. *IEEE Security and Privacy*, 9(3):56–59, May-June 2011.
[7] Wenliang Du and Ronghua Wang. Seed: A suite of instructional laboratories for computer security education. *J. Educ. Resour. Comput.*, 8(1):3:1–3:24, March 2008.
[8] D. Rowe, B. Lunt, and J. Ekstrom. The role of cyber-security in information technology education. In *Proc. ACM SIGITE*, pages 113–122, 2011.
[9] W. Sun, V. Katta, K. Krishna, and R. Sekar. V-netlab: An approach for realizing logically isolated networks for security experiments. In *Proc. USENIX CSET*, pages 5:1–5:6, 2008.
[10] UCSB. iCTF. http://ictf.cs.ucsb.edu/.
[11] UTSA. CCDC. http://www.nationalccdc.org/.
[12] Richard H. Wagner. Designing a network defense scenario using the open cyber challenge platform. Ms thesis, University of Rhode Island, 2013.
[13] Joseph Werther, Michael Zhivich, Tim Leek, and Nickolai Zeldovich. Experiences in cyber security education: The mit lincoln laboratory capture-the-flag exercise. In *Proc. USENIX CSET*, 2011.
[14] Michael E. Whitman and Herbert J. Mattord. The southeast collegiate cyber defense competition. In *Proc. 5th InfoSecCD*, pages 1–4, 2008.
[15] Le Xu, Dijiang Huang, and Wei-Tek Tsai. Cloud-based virtual laboratory for network security education. *IEEE Trans. Educ.*, 57(3):145–150, Oct. 2013.