Powering Hands-on Cybersecurity Practices with Cloud Computing

Ruipeng Zhang, Chen Xu, Mengjun Xie
The University of Tennessee at Chattanooga
Email: {smj793, kjx384}@mocs.utc.edu, mengjun-xie@utc.edu

***Abstract*—Cybersecurity education and training have gained increasing attention in all sectors due to the prevalence and quick evolution of cyberattacks. A variety of platforms and systems have been proposed and developed to accommodate the growing needs of hands-on cybersecurity practice. However, those systems are either lacking sufficient flexibility (e.g., tied to a specific virtual computing service provider, little customization support) or difficult to scale. In this work, we present a cloud-based platform named EZSetup for hands-on cybersecurity practice at scale and our experience of using it in class. EZSetup is customizable and cloud-agnostic. Users can create labs through an intuitive Web interface and deploy them onto one or multiple clouds. We have used NSF funded Chameleon cloud and our private OpenStack cloud to develop, test and deploy EZSetup. We have developed 14 network and security labs using the tool and included six labs in an undergraduate network security course in spring 2019. Our survey results show that students have very positive feedback on using EZSetup and computing clouds for hands-on cybersecurity practice.**

***Index Terms*—Cybersecurity Education; Hands-on Lab; Cloud Computing**

I. Introduction

As the scale of vacancy of cybersecurity jobs keeps rising [2] and cyber threats have become a new norm, recent years have witnessed a massive need for effective and affordable cybersecurity education solutions. As an indispensable part in cybersecurity education and training, hands-on practices have been particularly emphasized in addressing the shortage of cybersecurity workforce. However, it is challenging to implement hands-on cybersecurity practices at scale and in a cost-effective and flexible manner.

Traditionally, hands-on practices are locally set up on physical or virtual machines, which is time-consuming and error-prone. Meanwhile, these set-ups usually are not remotely accessible and have a problem of scaling up. With the advancement of virtualization technologies and software-defined networking (SDN), cloud-based cybersecurity practice platforms have emerged to address the scalability and availability issues of traditional methods. However, many of those systems are often tied to a specific virtualization technology (e.g., VMWare) and provide few user customization features. Moreover, they often incur significant costs or effort in deployment, hence hindering wide adoption of hands-on practices.

Here we present our experience of using an in-house developed, cloud-based education platform named EZSetup [4] for hands-on cybersecurity practices. EZSetup provides an open source solution that addresses scalability and customizability in cybersecurity practices and facilitates design and deployment of hands-on labs. A unique feature of EZSetup is that it supports simultaneous integration with multiple cloud providers. It also provides an interactive user interface (UI) for designing and managing system configuration and network topology. The NSF funded Chameleon cloud and a private OpenStack cloud have been used to develop and deploy EZSetup. We have developed 14 network and security labs on EZSetup. Six of them were applied in an undergraduate network security course in spring 2019. The class survey feedback on EZSetup and hands-on labs is quite positive. The students appreciate the 24/7 accessibility of those labs and zero effort in setting up labs.

978-1-7281-2700-2/19/$31.00 2019

II. Related Work

Cybersecurity practice tools that leverage virtualized environment have been extensively studied and developed in recent years. Based on the underlying infrastructure, these tools can be classified into three categories: hosted hypervisor-based, bare-metal hypervisor-based, and cloud-based. Hosted hypervisor-based tools such as SEED Labs [3] and OCCP (Open Cyber Challenge Platform) [8] use a hypervisor inside an operating system such as VirtualBox or VMware Workstation for setting up virtual environments. Bare-metal hypervisor-based tools including ISERink [6] and Platoon [5] are similar to hosted hypervisor-based tools except that their hypervisors directly run virtual machines on physical hardware. Cloud-based cybersecurity practice tools create cybersecurity practice environments at scale by interacting with public or private clouds. Examples of this type include V-Lab [9], DETER Lab [1] and EZSetup [4].

III. Design and Implementation

EZSetup simplifies the design and deployment of hands-on labs by offering an intuitive web-based UI and concealing cloud resource management operations in the back-end. The lab design completed in the UI is sent to the back-end through an API service, which instructs the environment builder to orchestrate cloud resources using vendor-specific APIs. Once the virtual networks and machine instances are up and running, the server configurator can install additional software dependencies and configure firewall policies. Finally, end users can access the lab and instances through the web UI or terminal. An overview

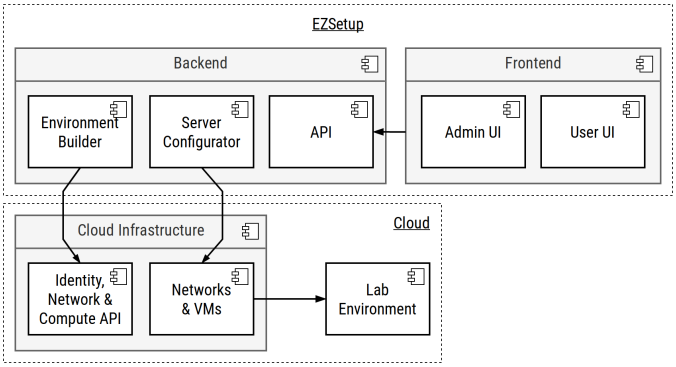

Fig. 1. System Architecture of EZSetup

TABLE I
14 LABS ON EZSETUP

Cloud Networking	Network Security	
(1) Linux Bridge	(7) TCP/IP Security	(13) VPN
(2) Open vSwitch	(8) Network Intrusion Detection	(14) Firewall
(3) OpenFlow	(9) Vulnerability Discovery	
(4) SDN Controller	(10) Mirai Botnet	
(5) Overlay Networks	(11) Web Security	
(6) Security Group	(12) Cross-Site Scripting	

of EZSetup's architecture is shown in Figure 1. More details about EZSetup can be found in [4].

The current version of EZSetup is implemented in Python 3 and JavaScript. Lab scenarios in EZSetup are implemented using a domain-specific language. They include basic server configuration such as boot image and network topology such as subnet IP spaces and security groups.

We have developed 14 labs on cloud networking and network security using EZSetup. Those labs are listed in Table I. Twelve of those labs have been available for free and public access on CLARK (https://clark.center), and the rest of them will be posted online soon. We have tested and deployed EZSetup and those labs on both private and public OpenStack clouds such as the Chameleon KVM cloud [7].

IV. EVALUATION

We applied EZSetup and the six labs we developed in an undergraduate network security coursed offered in spring 2019. Given access, resource and management considerations, we used a small private OpenStack cloud as the backend for EZSetup. The EZSetup server was running as an virtual instance in our cloud. Note that EZSetup can be deployed anywhere as long as it can access the cloud APIs. After the labs are instantiated, students can access the lab environment securely via OpenVPN connections.

At the end of the semester, we conducted an anonymous survey using 5 point Likert scale to collect students' feedback on the EZSetup lab environment and hands-on labs. The questions include:

Q1. My overall experience of using EZSetup is pretty good.
Q2. The labs are interesting to me.
Q3. I have been engaged in conducting the labs.
Q4. I am satisfied with the knowledge and skills I gained from the labs.
Q5. The overall level of difficulty of the labs is appropriate.
Q6. The lab instructions are useful.

The aggregated results of 13 collected survey answers are shown in Figure 2. The results clearly indicate that the overall feedback is quite positive regarding the usability of EZSetup and effectiveness of the cloud-based labs. More than 80% of the survey participants found that EZSetup is helpful in completing the lab tasks and the lab materials are informative. The results also show that on average about 38% of participants spent 2 to 4 hours in completing each lab and 62% of them spent 4 to 6 hours on each lab. The time spent on each lab and the comments and suggestions from the survey participants reflect that EZSetup successfully removed their burden on setting up lab environment and made them more focused on lab itself, hence making positive impact on their cybersecurity practices.

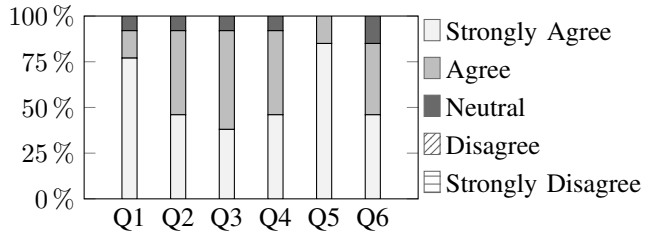

Fig. 2. Students' Answers to the Survey Questions

V. CONCLUSION

We have presented our experience of using EZSetup, an open-source cloud-based solution to cybersecurity practice, in an undergraduate network security course. Our survey results show that our cloud-based approach can make a positive impact on students' experiential learning and lower the barriers in promoting hands-on cybersecurity practices.

ACKNOWLEDGMENT

This work was supported in part by the NSF under grants 1338102 and 1623628, National Security Agency under grant H98230-17-1-0273. The development and testing of EZSetup used the NSF funded Chameleon cloud.

REFERENCES

[1] T. Benzel. The science of cyber security experimentation: The deter project. In *Proc. 27th ACSAC*, pages 137–148, 2011.
[2] I. Blog. Global cybersecurity outlook 2019, April 2019.
[3] W. Du and R. Wang. Seed: A suite of instructional laboratories for computer security education. *J. Educ. Resour. Comput.*, 8(1):3:1–3:24, Mar. 2008.
[4] Y. Li, D. Nguyen, and M. Xie. Ezsetup: A novel tool for cybersecurity practices utilizing cloud resources. In *Proc. SIGITE 2017*, pages 53–58.
[5] Y. Li and M. Xie. Platoon: A virtual platform for team-oriented cybersecurity training and exercises. In *Proc. SIGITE 2016*, pages 20–25.
[6] A. Luehm. Iseman: A management and deployment interface for lab-based activities within iserink. *Creative Components*, 2018.
[7] P. Riteau. New openstack kvm cloud available, September 2015.
[8] R. H. Wagner. Designing a network defense scenario using the open cyber challenge platform. Ms thesis, University of Rhode Island, 2013.
[9] L. Xu, D. Huang, and W.-T. Tsai. Cloud-based virtual laboratory for network security education. *IEEE Trans. Educ.*, 57(3):145–150, Oct. 2013.