ReScuE: A Cloud-based System for Cybersecurity Education and Training

Abstract - With the proliferation of the technology of virtualization, Software-Defined Network (SDN) and Network Function Virtualization (NFV), cloud computing has become a vital building block of the high-performance and low-cost computing paradigm serving for various educational purposes. In this paper, we first describe a free framework, namely *ReScuE* (Range for Security Education), which is a cloud-based networked virtual environment dedicated for cybersecurity education. We leverage the state-of-the-art technologies of SDN and NFV and elaborate the solutions to tackle the technical challenges of deploying ReScuE upon the underlying cloud infrastructure. Then, we present a set of hands-on labs that teach the students how to perform offensive, defensive, and forensic analysis tasks with the techniques and tools on the top of ReScuE. Finally, we tested both ReScuE and the hands-on labs with two groups of undergraduate students. Through the post-lab assessment and feedbacks, we gain some insights of how to effectively promote the wide adoption of the cybersecurity-related hands-on labs to the undergraduate- and graduate-level courses at different educational institutions (e.g., community colleges, 4-years universities, and post-graduate schools).

Keywords

Pervasive computing, Hands-on labs, Course module, CloudLab

1. INTRODUCTION

With the proliferation of the technology of virtualization, Software-Defined Network (SDN) and Network Function Virtualization (NFV), both industry and academia start to emphasize on building the high-performance, low-cost, and easy to maintain computing paradigm for various educational purposes. The increasing attention of Internet of Things (IoT) and Cyber-Physical Systems (CPS) introduces new security challenges and complications to the applications of Pervasive Computing. Equipping the students and the future workforce with the security knowledge and the technical skills to handle the challenges becomes a crucial task for the educators.

Although a big demand for qualified workforce embraces the future of Pervasive Computing, the availability of educational environment, curricula, and the hands-on labs, is still scarce due to several reasons. First, it is costly to maintain a well-equipped and dedicated environment for cybersecurity purposes at an educational institution. The fast evolution of computer technologies, however, requires that the highly adaptive technologies and tools to be used in the classroom with minimal cost. The recent advances of SDN and NFV offer the opportunity of using virtual artifacts to facilitate the cybersecurity education. Although cloud-based educational environments, such as National Cyber Range [2], DETERLab [10], EDURange [9], and the Seattle Testbed [3], have been developed, they are either dedicate for large-scale experiments or not free. The development of cloud-based virtual educational environments is still highly desired. Second, different from most virtual environments dedicated for teaching traditional computer science courses, the environment for cybersecurity hands-on practice requires some unique features, such as isolation, access control, intrusion detection, and prevention, etc. The general purposed virtual environments cannot directly be utilized to fulfill the security requirements for cybersecurity training purposes.

Last but not least, some large-scale cybersecurity experiments, such as botnet and DDoS attacks, involve a large number of computers, the sophisticated topology, and the real-world security setting. Unfortunately, it is difficult to conduct cybersecurity hands-on lab by using a simulator or an emulation environment, because the response of a simulated or an emulated system might be quite different from the real one. In addition, a significant amount of efforts are still needed to develop the emulated components. All these issues limit the development and the wide adoption of cybersecurity hands-on virtual environment.

To bridge the gap between the demand and provision, we design and implement *ReScuE* (Range for Security Education), a cloud-based system for cybersecurity education and training purposes. Building upon CloudLab [1] and leveraging the state-of-the-art technologies of SDN and NFV, ReScuE provides the key components and a user-friendly interface that allows the instructor to set up and maintain the virtual environment and monitor students' activities easily. To fully utilize the existing cloud infrastructure underneath, we tackle the technical challenges by deploying the virtual artifacts in parallel.

On the top of ReScuE, we develop a set of hands-on labs that teach the students how to perform offensive, defensive, and forensic analysis tasks with the techniques and tools. Both the ReScuE and the hands-on labs have been tested by two groups of undergraduate students. Through the post-lab assessment and feedbacks, we gain some insights on how to promote the wide adoption of the networked virtual environment and the cybersecurity-related hands-on labs to different educational institutions. We design multiple hands-on labs with the focus on security and privacy issues in pervasive computing, including mobile computing, vehicular ad-hoc network, and digital forensics. We have tested both the ReScuE and the hands-on labs with undergraduate volunteers from CS and IT majors. Through the post-

lab survey and feedbacks, we qualitatively assess the *efficiency* of the lab and the *effectiveness* of the labs in cybersecurity education.

In this project, we have made the follows major contributions.

- First, we have designed and implemented an open and free cloud-based framework, namely *ReScuE*, which is highly-scalable, highly-available, and highly-adaptable for various educational purposes. ReScuE leverages CloudLab, a public cloud infrastructure for the academic and educational purposes. In addition, we have developed the ReScuE Core library and a user-friendly interface with the OpenStack Python API [4], from which the instructor can easily manage the virtual assets and expand the functionalities of the framework.
- Second, we have developed a collection of course modules and hands-on labs that cover different security and privacy facets of pervasive computing, which includes SDN, NFV, Mobile Computing, and Forensic technologies and tools. Educators at different educational levels can develop their own materials and deploy hands-on labs upon ReScuE, which promotes collaboration and resource sharing.
- Third, we have conducted the formal assessment in a hands-on lab with two groups of undergraduate students. The assessment results show that most students are satisfied with the learning experience with the ReScuE and the hands-on lab. The assessment results also show that the learning outcomes have been achieved and the students became more enthusiastic in pursuing the cybersecurity-related careers in the future.

The remainder of the paper is organized as follows. In Second 2, we present the system architecture of ReScuE. In Section 3, we describe the developed cybersecurity-related hands-on labs, with the focus of one example hands-on lab. The assessment procedure, results, and their

analysis are presented in Section 4. Finally, we conclude the paper and discuss the future work in Section 5.

2. SYSTEM DESIGN OF RESCUE

Figure 1 illustrates the system architecture of ReScuE, which contains three major components: 1) The ReScuE Core Library, which provides the major functionalities of constructing, managing, backing up, and restoring the cloud-based networked virtual environment; 2) the web-based user interface, which allows the students to sign up and obtain the information about the virtual artifacts. It also allows the instructor to monitor the current usage of the virtual artifacts by the students; 3) the command line interface (CLI), which allows the instructor to manage the environment through the ReScuE Core Library.

ReScuE significantly enhances the existing capability of the CloudLab and the default functionalities provided by OpenStack web interface by specifying the following key components:

- Each cybersecurity-related experiment is assigned with a *workspace*, which consists of multiple *Security Groups* (SGs). We define the SGs for the purpose of preventing the vandalism of malicious users and the abuse of novice users. Since each SG is self-contained, the lab tasks in an SG can be accomplished without interfering other SGs. A student can access the assigned VMs or containers in an SG via the SSH client software or the WebSocket-enabled browser console.
- Each student is assigned an independent security group, in which the offensive tasks can be performed from the *Attacking Domain* (AD) and the defensive/detective/forensics tasks can be performed from the *Target Domain* (TD).
- The security policy is set up such that 1) the VMs in the attacking domain and the target domain can access each other; 2) the ingress traffic can only be forwarded to the VMs in the attacking domain and target domain from the NAT server; and 3) the egress traffic cannot be

forwarded from the attacking domain and target domain to the outside of the security group.

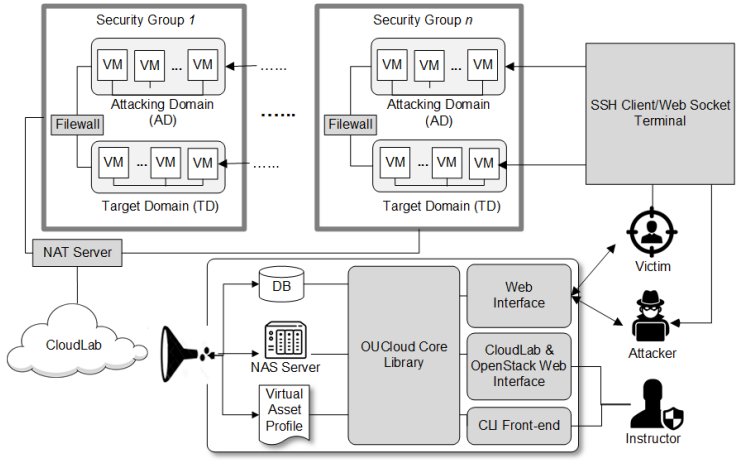


Figure 1: The system architecture of ReScuE and its key components.

ReScuE interacts with both the instructors and the students through three major services: 1) *User Management*, 2) *Virtual Environment Management*, and 3) *Infrastructure Management*. In particular,

- The service of user management oversees the current users of the virtual environment. It maintains the information of user signup/login, assigns the resources, such as the IP addresses and the security groups to the users, and reclaims the resources after the usage.
- The service of virtual environment management maintains the virtual assets in a virtual environment. Its key functionalities include creating and updating the networked virtual environment, backing up/restoring the virtual environment, uploading and downloading the VM/container images, and creating and configuring the security groups. To facilitate the backup and restore of the virtual environment, we use the term of the *profile* to describe a collection

of information that is necessary to construct a virtual environment, whose detail will be presented in Section 2.1.

- The service of infrastructure management retrieves the configuration data from the CloudLab and the OpenStack instance and uses them as the parameters to configure ReScuE.

2.1 The Management of the Virtual Artifacts

One important design goal of ReScuE is to make the entire networked virtual environment easy to set up, easy to maintain, and highly scalable so that it can achieve the wide adoption. The instructor should merely focus on the application logic of a virtual environment without knowing the physical machine beneath it.

To achieve this goal, the ReScuE overcomes several technical challenges under the current provision of CloudLab. First, the CloudLab does not provide the persistent storage, such as the hard drive and solid-state drive for a long-term (e.g., several weeks or months). It may cause the inconvenience to both the instructor and students if they want to keep the environment for a long time, review the results of the exploits, and replay the exploits again in the same network setting. To solve this problem, we attach ReScuE with the Network-Attached Storage (NAS) server hosted at Oakland University, which allows the entire networked virtual environment, including the profile, the VM/container images, and their snapshots to be stored permanently offline. Even the CloudLab reclaims the physical resources that host all the virtual artifacts, the data saved on the ReScuE can always allow the entire virtual environment to be reconstructed easily.

As previously mentioned, we use a collection of information (the virtual artifacts and their attributes) that is necessary to construct a virtual environment as the profile of the environment. Table 1 lists a subset of the virtual artifacts and their attributes (as the XML elements) used in the profile. Without otherwise noted, all the listed artifacts are *virtual*.

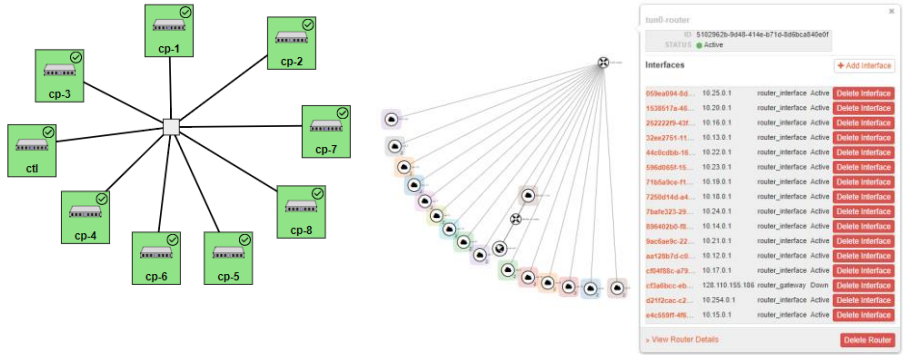
Table 1. A subset of virtual artifacts and their attributes (as the XML elements) used in the profile.

Virtual Artifacts	**XML Elements**	**XML Attributes**
Networks	<Networks>	<Network_ID>, <Network_Name>, <Network_Admin_State_UP>, <Subnet_ID>, <Subnet_Name>, <Subnet_CIDR>, <Subnet_IP_Version>, <Subnet_GateWay>
Network Interfaces	<Interfaces>	<Interface_ID>, <Network_ID>, <Interface_Admin_state_UP>, <Connected_Device_ID>, <InterfaceSubnet_ID>, <IP>
Routers	<Routers>	<Router_ID>, <Router_Admin_State>, <Zone>, <Interface_ID>, <Floating_IP>
Virtual Machines	<Images>	<Image_Name>, <Container_Format>, <Disk_Format>
	<Flavors>	<Flavor_Name>, <VCPU>, <Disk>, <RAM>
	<Instances>	<Instance_ID>, <Name>, <Status>, <Flavor>, <Image>, <Interface_ID>, <IP>

2.2 Performance Challenges and The Corresponding Solutions

Although CloudLab provides powerful physical machines and is capable of balancing the workload when constructing the virtual environment, we

observe a significant delay when the virtual environment is large. More specifically, we made two important observations: First, we found that the major bottleneck of constructing the virtual environment is due to the fact that the controller (CTL) issues the OpenStack commands of creating the virtual artifacts on the computer (CP) in serial. Second, there is no explicit data dependency of constructing the virtual artifacts on each physical computer. Thus, it is possible to construct virtual artifacts and virtual network on multiple nodes in parallel.



(A) The topology of a sample experiment with 9 physical machines.

(B) The networked virtual environment with 14 security groups.

Figure 2: The deployment of a sample experiment by using ReScuE.

Based on these observations, we develop a parallel solution of deploying a large-scale virtual environment crossing multiple CPs. More specifically, we defined and implemented two levels of parallelism: *intra-network* and *inter-network* parallelism. For intra-network parallelism, we create the VMs that share the same network environment but have no interdependence in parallel. For inter-network parallelism, we create the virtual network that is deployed on each physical CP but have no interdependence in parallel. Figure 2 visualizes the parallel construction of a virtual environment of 14 security groups with 9 physical computers.

To evaluate the performance speed-up of using these two levels of parallelism, we measure the time of creating the virtual network with a different number of VMs and threads. Figure 3 shows the comparison of

the performance for different settings. In this experiment, we use 9 physical machines, in which one is the CTL, and the other 8 are the CPs. Each machine has 20 virtual CPU cores, 64 GB memory, and 480 GB SSD storage. Each VM has one virtual core, 1 GB memory, and 20 GB disk space. As shown in the diagram, regardless of the number of the networks, the time spent is decreasing when the number of the threads increases. This result indicates at least two insights: First, there is a significant decrease when the number of threads reaches to 8, which is equal to the number of the physical CPs. Second, the increasing number of threads have a more significant impact to construct a larger scale network. For example, the time elapsed to create 64 networks with 64 threads is less than 400 seconds, while the time elapsed to create 32 networks with one thread is more than 500 seconds. It is obvious the parallelism improves the performance of constructing the virtual environment.

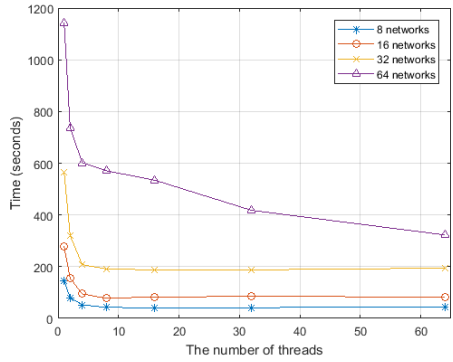


Figure 3: The elapsed time for constructing the virtual environment with different settings.

3. AN EXAMPLE EXPERIMENT

We have designed and implemented four hands-on labs, which cover the security concepts and practice of pervasive computing as illustrated in Table 2. They emphasize on different disciplines of the pervasive computing, including cloud computing, mobile computing, and IoT

computing. Due to the space limit, we only focus on the details of one lab in the following subsection.

Table 2. The list of the cybersecurity-related hands-on labs.

Labs	Title
1	Cloud-based malware construction and virtual machine introspection
2	Fine-grained access control with Attribute-based Encryption (ABE)
3	Processing encrypted data with Homomorphic Encryption (HE)
4	The SQL injection attack for mobile devices

3.1 Cloud-based Exploits Construction and VM Forensic Lab

In this lab, the student will learn how to use the off-the-shelf tool, including using the open-source tools to perform vulnerability discovery, exploit, and forensic investigation, respectively. We also created the customized VMs as the attacking VM and the victim VM for the experiment. The detailed learning objectives are the following:

- Be able to apply the vulnerability discovery tool, such as OpenVAS [6], to discover the software vulnerabilities.
- Be familiar with the exploit technologies and be able to apply the tool, such as Metasploit Framework (MSF) [5], to construct the exploits.
- Be familiar the memory forensic technologies and be able to apply the tool, such as Volatility [7], to introspect the VM images and discover the virtual artifacts for forensic investigation.

The roadmap of this hands-on lab is illustrated in Figure 4.

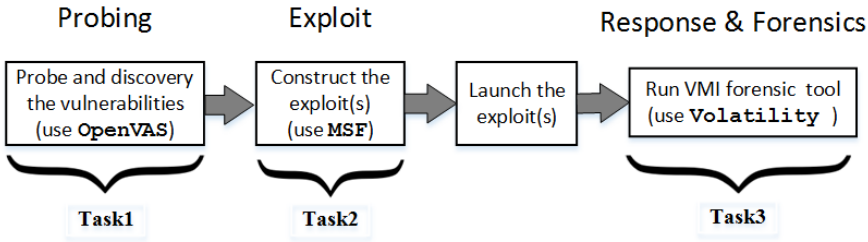


Figure 4: The roadmap of a hands-on lab.

In order to obtain the VMs for the experiments, students are required to log in to the web portal of ReScuE. Figure 5 illustrates the web-based interface of ReScuE. In particular, Figure 5 (A) illustrates the login page of ReScuE and Figure 5 (B) illustrates the information of the VMs used in the experiment. Students can use either *MobaXterm* or the WebSocket to access the VMs.

(A) The login/signup page of ReScuE.

(B) The information of the VMs used in the experiment.

Figure 5: The web-based user interface of ReScuE.

4. EVALUATION AND RESULT ANALYSIS

The course modules and the hands-on labs were piloted by two groups of undergraduate students. One group of students, namely *UG1*, came from our university's "Undergraduate Computer Researcher (UnCoRe) in Secure and Trustworthy Cyberspace" (OU's REU program). The other group of students, namely *UG2*, came from the junior and senior level students, who are taking the course "Information Security Practice". All students in these two groups participated in this project after the debriefing of the objective of the project and their involvements are voluntary-based. All students completed the pre- and post-surveys.

4.1. Statistics of Students Sample

There are a total number of 18 students participated in the assessment. The statistics of the participants are listed in Table 3.

Table 3. The statistics of the participants in our evaluation.

	UG1 – Date: 07/13/2017	**UG2 – Date: 03/10/2018**
Gender	Male: (9) Female: (1)	Male: (7) Female: (1)
Ethnicity	White: (8) African American: (1) Hispanic: (1)	White: (3) Asia: (5)

4.2. Data Analysis and Result Evaluation

We use the similar evaluation taxonomy used in the literature [8] to qualify the *efficiency* of the lab and the *effectiveness* of the labs in cybersecurity education. To quality the efficiency of the lab, which focus on the appropriateness of the lab, we use the following metrics:

- The clarification/usefulness of the lab instruction and the supporting materials;
- The usability of the virtual environment;
- The amount of time that students spent in the lab;
- Whether the time spent is worthwhile; and
- The overall satisfaction of the lab.

In addition, to assess the effectiveness of the labs in cybersecurity education, which focus on the students' learning as a result of the lab, we use the following metrics:

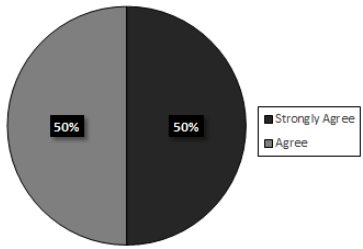
- The level of challenge presented by the lab exercise;
- The familiarity of knowledge and skills before/after the lab; and
- The level of students' interests in the lab exercises.

We conducted an anonymous survey after students finished the labs. The survey questions are multiple-choice questions and open questions. Nevertheless, we ask students the two open questions:

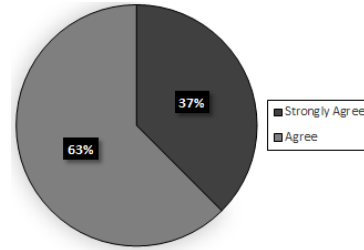
- *Which part of this lab could be improved?*
- *Which part of the virtual environment could be improved?*

4.3. Data Analysis and Results Evaluation

The first set of assessment measures the students' satisfaction towards usability of the ReScuE. Figure 6 shows that all students in both groups (UG1 and UG2) are either strongly agree or agree that the ReScuE is easy to use. It clearly indicates that ReScuE is applicable to the cybersecurity-related hands-on lab.



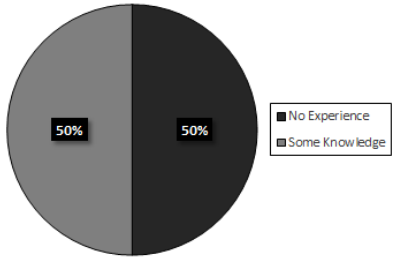
(A) The result of UG1.

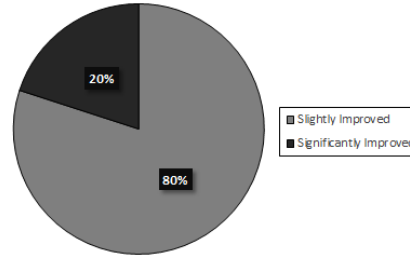


(B) The result of UG2.

Figure 6: Students' response to the question "The environment to access the VM is easy to use."

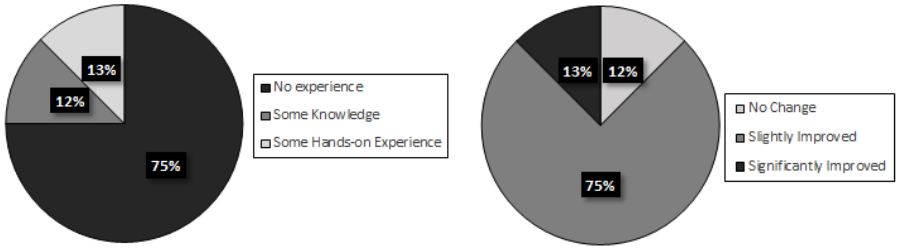
The second set of assessment measures whether the students' knowledge and skills increased significantly after the lab. Figure 7 and Figure 8 show the statistics of students' self-efficiency of their familiarity with the cybersecurity-related knowledge *before* and *after* the hands-on lab. Both groups reported an increase in self-efficiency beliefs after exercising with the lab. In particular, all the students in the UG1 responded that their level of familiarity increases slightly or significantly after taking the hands-on lab; while 88% of the students in the UG2 answer that their level of familiarity increases slightly or significantly after taking the hands-on lab. It is worthwhile to note that, 50% of the students in UG1 and 75% of the students in UG2 have no cybersecurity experience before taking the hands-on lab. Therefore, the improvement of the self-efficiency is significant.





(A) The level of familiarity before the lab. *(B) The level of familiarity after the lab.*

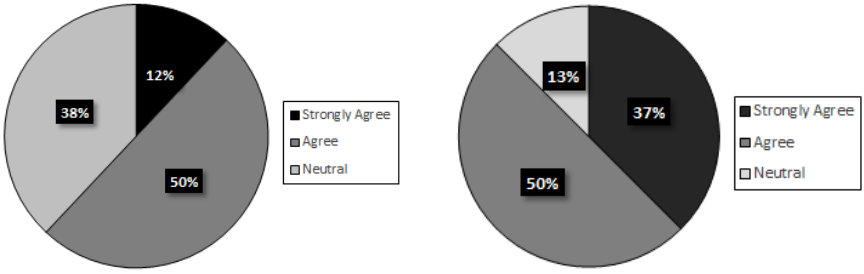
Figure 7: Students' response to the questions "The level of familiarity in the cybersecurity -related knowledge before/after the lab" from UG1.



(A) The level of familiarity before the lab. *(B) The level of familiarity after the lab.*

Figure 8. Students' response to the questions "The level of familiarity before/after the lab" from UG2.

The third set of assessment measures the improvement of students' interests in cybersecurity after taking the hands-on lab. The results show that 62% of the students in UG1 and 87% of the students in UG2 agree that the hands-on lab makes them become more interested in cybersecurity after taking this lab.



(A) The result of UG1. *(B) The result of UG2.*

Figure 9: Students' response to the question "I became more interested in cybersecurity after taking this lab."

The students from both groups provide constructive feedback towards the lab instruction and the ReScuE. For instance, one student commented, "Please provide more information on what is being done when running the exploits and what vulnerabilities are being exploited." This motivates us to provide more detailed information in an introductory lecture and/or the supporting materials for our students to read before taking the lab. For the feedback of how to improve the ReScuE, most of the students' suggestions focused on the usability of the website, such as adding the functionality of spelling checking and email authentication.

5. CONCLUSION AND FUTURE WORK

With the proliferation of the technology of virtualization, SDN, and NFV, cloud computing has become an important technology that facilitating educational purposes. In this paper, we describe *ReScuE*, a cloud-based networked virtual environment dedicated to cybersecurity education. ReScuE leverages a free cloud infrastructure and solves some technical challenges in the infrastructure. We have also developed the cybersecurity-related hands-on labs upon which students can conduct offensive, defensive, and forensic experiments. The framework and the hands-on labs have been tested by the students. The assessment results show that ReScuE improves the students' proficiency in the knowledge and skills, as well as increases their interests in cybersecurity.

Future research and the cybersecurity workforce training can be conducted in the following ways. First, we will evaluate the effectiveness and the impact of our current curricula in a larger scale for the purpose of improvement. Specifically, we will adopt and inject the course modules and the hands-on labs to both the undergraduate- and graduate-level courses to benefit a broader range of students. Second, we will design and implement a user-friendly web interface for the educator to construct the virtual environment easily and make it public. Educators can use the public platform to design the new course materials, set up the special-

purpose virtual environment, and upload customized VM/container images onto ReScuE. Third, we will design and implement more hands-on labs. Finally, we will present ReScuE at different educational institutions (e.g., community colleges, 4-year universities, and post-graduate schools) and collect the feedback from the community of cybersecurity education.

6. ACKNOWLEDGMENT

This work is partially supported by the National Science Foundation under awards Grants No. DGE-1723707, DGE-1623713, CNS-1460897, and the Michigan Space Grant Consortium. 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 also thank Melissa Nichols, Nathan Torrez, Hisham Kanaan, and Tianhuan Tu for their constructive discussion and prototype implementation.

REFERENCES

[1] The CloudLab Project. (2018). Retrieved from https://www.cloudlab.us/.

[2] National Cyber Range (2018). Retrieved from https://www.acq.osd.mil/dte-trmc/ncr.html

[3] The Seattle Testbed (2018). Retrieved from https://seattle.poly.edu/html/

[4] A. Shrivastwa, S. Sarat, K. Jackson, C. Bunch, E. Sigler, and T. Campbell. (2016). *Openstack: Building a Cloud Environment*. Packt Publishing.

[5] Metasploit Framework Project. (2018). Retrieved from https://www.metasploit.com/

[6] OpenVAS. (2018). Retrieved from http://www.openvas.org/

[7] Volatility. (2018). Retrieved from http://www.volatilityfoundation.org/

[8] W. Du and R. Wang. (2008). SEED: A Suite of Instructional Laboratories for Computer Security Education. *ACM Journal on Education Resources in Computing*. Vol. 8, Issue 1, pp. 3:1 - 3:24.

[9] R. S. Weiss, S. Boesen, J. F. Sullivan, M. E. Locasto, J. Mache, and E. Nilsen. (2015). Teaching Cybersecurity Analysis Skills in the Cloud. In *Proceedings of the 46th ACM Technical Symposium on Computer Science Education* (SIGCSE '15). ACM, New York, NY, USA, pp. 332 - 337.

[10] P. A. Peterson and P. L. Reiher. (2010). Security Exercises for the Online Classroom with Deter. In *Proceedings of 3rd USENIX Workshop on Cyber Security Experimentation and Test.* pp. 73 - 76