Cloud Deployment Support for Cybersecurity Training

1810427 ZHANG ZHE

In recent years, cloud computing technology has received considerable attention from various fields, playing a vital role in all walks of life. Cybersecurity is always a hot research topic. With the introduction of the cyber range concept, more and more cybersecurity education and training systems have been developed. But most of these systems are implemented on the local computer and server. Although there are many existing cloud-based cybersecurity systems developed in recent years, there are limited researches on how to transform those classic cybersecurity education and training systems into cloud deployment.

Thanks to the current market competition in cloud computing, various cloud vendors have introduced different welfare policies to attract users. This makes it easier for everyone to get the opportunity to use cloud computing services. After comparing the use threshold of some cloud computing platforms (e.g. AWS, Azure, Google Cloud), we have found that the AWS educate account jointly launched by AWS and Vocareum (a third-party service as a manager) is very suitable for research, development, and testing. Thus, we applied for an AWS educate account and used it in our research.

For the research, we proposed an approach to introduce AWS cloud computing into an open-source system named CyRIS (Cyber Range Instantiation system), so that cyber range can be deployed in the AWS cloud platform. CyRIS generates cyber range based on the description file in YAML format automatically on the computer and network infrastructure, the description file includes environment settings and security content. This CyRIS process can be divided into three parts, base VM preparation, content installation, and guest VM cloning. We used EC2(Amazon Elastic Compute Cloud) services to replace the KVM-based phase of base VM preparation and guest VM cloning through the Python SDK Boto3 of AWS (CyRIS is developed based on Python).

In our experiment, firstly, we completed the installation of the original CyRIS to ensure that there are no problems with the environment and programs, and then we prepared the AWS development environment, which includes account registration, import of credentials information, and SDK installation. On the method proposed, we used EC2 service to create instances as base VMs. Then we proceed to the content installation phase. Since the target machine is in the cloud, we have made adjustments to the content installation part of the source program, such as modifying the SSH login method, modifying the commands of individual tasks, and so on. During the cloning step, we stop the instances that the content has been installed

before, and create AMIs (amazon-based image) based on the instances. According to the specified number of clone settings in the description file, launch the instances with the newly created AMIs. How to run the improved CyRIS is basically the same as before. After ensuring that the original CyRIS can run normally, log in the credentials information and run the improved CyRIS program. Then users can get the range notification from the specified directory, according to the information in the range notification, users can access the cyber range.

To evaluate the performance of our improved system, we first conduct a review of the operating status of AWS services. We created a uniform specification cyber range several times per hour of the day and collected all creation time data. Then we calculated the average and standard deviation of each hour's creation time to compare the efficiency and stability of cyber range creation on AWS for finding a suitable time period to create cyber ranges. We create cyber range of different specifications during these times and compared the total cyber range creation time with the original CyRIS. Besides, we compare the details of the time for both kinds of CyRIS. Finally, the performance is analyzed and evaluated through line charts and bar plots with error bars.

Based on the comparison results, we proved that cloud-based CyRIS has higher efficiency while creating multiple base VMs. In addition, the improved CyRIS can use more operating systems for the base VMs because of the convenience that the instance can be launched only through AMI id on the AWS platform. Through the improvement of the source program, the original installation contents are supported in more operating systems (e.g., Red Hat 8, Ubuntu 20.04, Amazon Linux) and almost all of the contents work well. We adjusted the source program to make some tasks that were originally only available on CentOS7 available on all of our AMI operating systems in AWS cloud, such as emulate attacks, emulate malware, and modify firewall rules.

However, we have also discovered some limitations in our experiment. The AWS educate account has some restrictions. It can not keep more than nine instances running at the same time, so we are not able to evaluate the situation of creating big scale cyber range. And due to account restrictions, we unable to confirm how much the used cloud services cost, etc. Besides, because of some security policies of the cloud platform, the real attack emulation task in the original system cannot be inherited by the improved system.

In summary, our research has successfully improved CyRIS so that it can deploy cyber range on the AWS cloud platform based on the description file in the YAML format. And the method we proposed can also provide some reference value to other classic cybersecurity education and training tools or

systems for cloud deployment and conversion.

In future work, we plan to add more installation content to enrich CyRIS. We will also apply for a general AWS account, which has lifted the previous educate account restrictions so that we can make more improvements and tests. For example, we can evaluate the situation of cyber range creation in more kinds of scales. And we can use more AMI from the AWS marketplace. For more secure and reliable user login, we plan to create a separate key pair for each cloned instance in future improvements.