Automated Deployment of Cybersecurity Labs in Cloud Computing Environments

Emergent Research Forum (ERF)

Christopher Simpson
Dakota State University
ctsimpson25692@pluto.dsu.edu

Omar El-Gayar
Dakota State University
Omar.El-Gayar@dsu.edu

Dave Bishop
Dakota State University
Dave.Bishop@dsu.edu

Abstract

Government and private sector reports continue to highlight the shortage of qualified cybersecurity professionals. Hands-on cybersecurity labs can enhance student learning and augment the gap in qualified teachers. While there is a large body of research on cybersecurity labs, it is challenging to recreate these labs due to the use of proprietary software, significant hardware requirements, or large data transfer requirements. The automated deployment of IT infrastructure allows for the easy deployment and sharing of lab environments. This research proposes a framework for the use of DevOps tools to automate the deployment of cybersecurity labs that maps to specific learning objectives. We apply design science research methods to create a proof of concept demonstration that automates the deployment of the same cybersecurity lab environment on two different cloud providers. The research provides a new framework and method to create, deploy, and share cybersecurity labs that are mapped to learning objectives.

Keywords

Cybersecurity, education, labs, DevOps, cloud.

Introduction

A 2017 government report noted the need for a highly trained workforce and specifically recommended that the "Private and public sector organizations should sponsor the use of virtual training and assessment environments to augment the limited cadre of teachers and assessment tools that match workforce needs" (Ross and Duke 2017). The report also noted the need for "hands on and experiential learning" (Ross & Duke, 2017).

The rapid growth of virtualization and cloud computing technologies allow for the programmatic deployment of information technology (IT) infrastructures using automated deployment tools and common software repository management tools. The terms DevOps and "infrastructure-as-code" are commonly used to describe this automation process (Artac et al. 2017). While there is a large body of research on cybersecurity labs, it is challenging to recreate these labs due to the use of proprietary software, significant hardware requirements, or large data transfer requirements. The automated deployment of IT infrastructure allows for the easy deployment and sharing of lab environments.

DevOps provides a framework for the automated and programmatic deployment of IT resources in virtualized and cloud computing environments (Ragan 2013). The DevOps construct also supports continuous integration and continuous deployment of software and IT updates (Rathod and Surve 2015). Under the DevOps construct, infrastructure is be treated as code in a cloud or virtualized environment and is managed with standard software source code control and revision management tools (de Bayser et al. 2015).

The purpose of this research is to explore the use of DevOps tools to create and deploy cybersecurity labs to enhance student learning and allow for increased sharing of cybersecurity lab environments. The research proposes a framework for the use of DevOps tools to automate the deployment of learning objective driven, cloud-based cybersecurity labs that are based on learning theory to improve student outcomes. This research examines available DevOps tools and will select the best ones to build a proof of concept. The objectives and tasks are based on the NICE Workforce Framework and the NSA CAE Knowledge units (NIETP 2018; Paulsen et al. 2012). Following a design science research guidelines (Hevner et al. 2004) and process (DSRP) (Peffers et al. 2006) the next section provides a review of the literature highlighting the research gap and its significance. Next, we present the objective of the solution followed by the proposed model to lab deployment via DevOps. The evaluation section discusses the evaluation of the proposed artifact. The last section concludes the paper with a summary, and directions for future research.

Literature Review

One of the major goals of cybersecurity education is to prepare students for the workforce. Similar to competitions, hands-on labs allow students to develop real-world skills required in the field (Manson and Pike 2014). With the constructivist approach, learners solve "meaningful" and "realistically complex" problems to construct knowledge (Tam 2000). Floyd and Yerby (2014) applied constructivist theory to the development of digital forensics labs. Active learning makes students active participants in their learning and allows them to "lean by doing" (Chatmon et al. 2010; Paulson and Faust 1998). There are several techniques such as collaborative learning, Problem-Based Learning, and Learning by Doing that support active learning (Nieweg et al. 2005; Paulson and Faust 1998).

The use of cybersecurity labs in education was discussed at the first ACM workshop on education in computer security (Irvine 1997). Early research into the development of labs noted the challenges of creating and maintaining labs (Mateti 2003). The use of hands-on cybersecurity labs allows students to apply theory in a safe environment (Schweitzer et al. 2009). The use of these labs provide for an active learning environment that supports student participation and can increase student motivation and retention (Floyd and Yerby 2014; Schweitzer et al. 2009).

The use of virtualization is a common theme in the research related to the development and deployment of cybersecurity labs (Chen and Tao 2011; Fulton 2011; Haag et al. 2011; Padman and Memon 2002; Subrata Acharya and Ryoo 2010). Subrata and Ryoo propose a template model for the design and development of virtualized labs (2010). Fulton and Schweitzer also highlight the challenges of creating and deploying labs and the complexity of managing the configuration of and administering virtual machines (Fulton 2011). More recent research identifies the use of cloud computing platforms for the delivery of cybersecurity lab environments (Alexander et al. 2012; Geigle et al. 2018; Weiss et al. 2014; Xu et al. 2014). The ADLES specification language and deployment system provides a method to abstract the creation of virtual machines for hands on cybersecurity labs (Conte de Leon et al. 2018).

While there has been significant research and development of lab environments, with few exceptions, access to the different lab environments are proprietary, require specific software, or require registration with the developer of that environment. For example, Xu et al. present an excellent lab environment but don't offer a method to replicate this environment. These barriers may prevent an institution from accessing a specific set of labs. Development of a lab configuration framework will remove these barriers and allow access to more lab environments. Geigle et al. provide a good example on the use of DevOps tools for continuous integration and version control for lab environments in the context of data science (2018).

Objectives of the Solution

The main objective of the solution (framework) is the ability to map learning objectives and tasks to system configurations, i.e., facilitating the process for mapping security curriculum to lab content that can be used for cybersecurity classes at the graduate and undergraduate levels. The use of DevOps tools to programmatically alter lab content supports customization of labs based on student level and program of study. Embedding objectives and tasks into the lab creation and deployment process will allow educators to use labs that are relevant to their curriculum and find lab content that best fits their requirements. The

set of objectives and tasks will be based on commonly accepted standards (NICE Framework and CAE Knowledge Units).

A second objective is to evaluate DevOps constructs to automate the creating and deployment of these labs and demonstrate the labs can be easily shared across multiple cloud environments. The DevOps construct and associated tools are platform agnostic. Use of these tools for the creation of cybersecurity labs will allow the deployment of labs across multiple cloud environments. The configuration files for each of these tools are not compatible; however a higher-level descriptive framework would allow the translation of configurations for use with either tool. Use of automated DevOps tools for the configuration and deployment of the lab environments allow the instructor to focus on developing the content rather than manually configuring the various virtual machines. For example, the lab environments created by Chen and Tao could be replicated onto different cloud platforms using DevOps tools (2011).

Framework

The constructivist theory of learning will be applied to develop the artifacts of this research to support active and problem-based learning. The proposed framework will take learning objectives and map those objectives to specific virtual machine configurations. Those configurations will be deployed to cloud based virtual machines using DevOps methods and tools. A web-based frontend will allow instructors to select desired objectives to create custom deployments. Figure 1 is a high-level system description of the lab creation method. Figure 2 shows an example of the process for mapping learning objectives and tasks to the creation and deployment of a virtual machine.

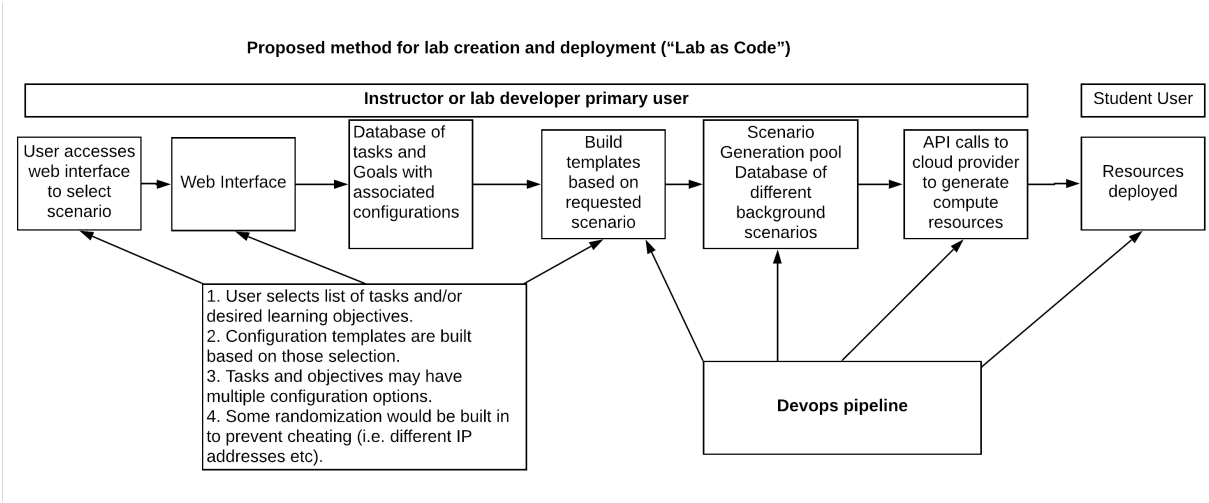

Figure 1 High Level System Description

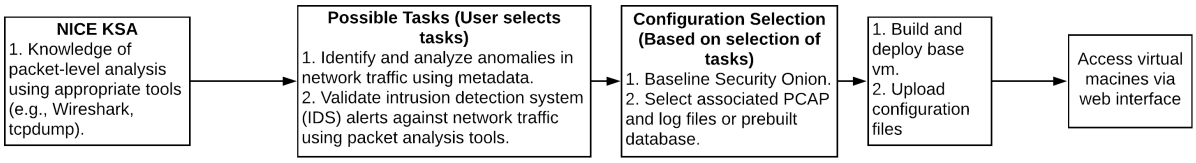

Figure 2 Learning Objectives to VM Creation Map

An architecture for a supporting DevOps-based system for the deployment of cybersecurity labs is briefly described as follows:

Web Interface: Provide front end GUI for the selection of objectives and tasks.

Learning Objective Database: A database that contains cybersecurity related learning objectives. Each objective will be mapped to one or more tasks.

Tasks Database: The tasks database will contain mapping of cybersecurity related tasks that meet learning objectives. The tasks will be linked to either a pre-built template or a configuration item.

Configuration Repository: This repository will contain baseline configurations, pre-built templates, and build instructions that are mapped to specific tasks.

Credential Repository: This secure repository will contain the users access keys and credentials for the deployment of the selected infrastructure on the desired cloud provider.

Evaluation

The initial instantiation will be a proof of concept web-based front-end that allows instructors to select a set of student learning objectives and tasks. These objectives and tasks will be mapped to lab configurations and used to create and deploy a lab environment with DevOps deployment tools on two different cloud providers. This instantiation will include:

1. A repository of learning objectives mapped to tasks.
2. A repository of tasks mapped to pre-built templates and configuration items.
3. A library of templates and configuration items that support specific tasks and objectives.

The proof of concept deployment will be developed to support a constructivist learning environment and will be guided by the instructional principles described by Savery and Duffy (1995). Instructors will be able to select learning objectives that will create and deploy labs based on the indicated learning objectives, engage the learner in tasks that are part of a larger problem, and provide the learner ownership in developing a solution (Savery and Duffy 1995).

The proof of concept will include one lab that is an attack scenario and one lab that is a defensive scenario. Each lab will be mapped to a minimum of two NSA CAE Knowledge units and a minimum of five NICE Framework Knowledge, Skills, Abilities, and Tasks (Newhouse et al. 2017; NIETP 2018).

Summary and Future Research

There is a wide body of research on the development and use of hands-on labs for cybersecurity education and an emerging body of knowledge on the automated deployment of IT infrastructure into cloud environments. This research will address the limitations of sharing lab environments and provide a theoretical framework to automate the creation and deployment of cybersecurity labs based on learning objectives into cloud computing environments. The practical contribution of this research will be proof of concept lab deployments into different cloud computing environments. These proof of concept deployments will be evaluated by lab administrators, lab developers, and lab users. Future research will include the automated assessment of labs and the randomizing of some configuration parameters to prevent cheating without compromising the objectives of the lab.

REFERENCES

Alexander, J., Dick, A., Hacker, J., Hicks, D., and Stockman, M. 2012. "Building a cloud based systems lab," in: Proceedings of the 13th annual conference on Information technology education. Calgary, Alberta, Canada: ACM, pp. 151-154.

Artac, M., Borovssak, T., Nitto, E. D., Guerriero, M., and Tamburri, D. A. 2017. "DevOps: Introducing Infrastructure-as-Code," 2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C), pp. 497-498.

Chatmon, C., Chi, H., and Davis, W. 2010. "Active learning approaches to teaching information assurance," in: 2010 Information Security Curriculum Development Conference. Kennesaw, Georgia: ACM, pp. 1-7.

Chen, L.-C., and Tao, L. 2011. "Teaching Web Security Using Portable Virtual Labs," in: 2011 11th IEEE International Conference on Advanced Learning Technologies (ICALT). IEEE, pp. 491-495.

Conte de Leon, D., Goes, C. E., Haney, M. A., and Krings, A. W. 2018. "ADLES: Specifying, deploying, and sharing hands-on cyber-exercises," Computers & Security (74), pp. 12-40.

de Bayser, M., Azevedo, L. G., and Cerqueira, R. 2015. "ResearchOps: The case for DevOps in scientific applications," Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium

on, pp. 1398-1404.
Floyd, K., and Yerby, J. 2014. "Development of a digital forensics lab to support active learning," SAIS, pp. 14-2014.
Fulton, S. 2011. "A Concept Focused Security Lab Environment," Colloquium for Information Systems Security Education), pp. 1-6.
Geigle, C., Lourentzou, I., Sundaram, H., and Zhai, C. 2018. "CLaDS: a cloud-based virtual lab for the delivery of scalable hands-on assignments for practical data science education," in: Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education. Larnaca, Cyprus: ACM, pp. 176-181.
Haag, J., Horsmann, T., Karsch, S., and Vranken, H. 2011. "A distributed virtual computer security lab with central authority," CSERC '11 Computer Science Education Research Conference, Heerlen, The Netherlands: Open Universiteit, Heerlen, pp. 89-95.
Hevner, A. R., March, S. T., Park, J., and Ram, S. 2004. "Design science in information systems research," MIS Quarterly (28:1), pp. 75-105.
Irvine, C. E. 1997. "The first ACM Workshop on Education in Computer Security," ACM SIGSAC Review (15:2), pp. 3-5.
Manson, D., and Pike, R. 2014. "The case for depth in cybersecurity education " ACM Inroads (5:1), pp. 47-52.
Mateti, P. 2003. "A laboratory-based course on internet security," ACM SIGCSE Bulletin: ACM, pp. 252-256.
Newhouse, W., Keith, S., Scribner, B., and Witte, G. 2017. "NIST Special Publication 800-181 National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework." pp. 800-181.
NIETP. 2018. "CAE-CD 2019 and Beyond Knowledge Units (KUs) (Effective Fall 2018)." from https://www.iad.gov/NIETP/CAERequirements.cfm
Nieweg, M. R., Saunders-Smits, G. N., and Graaff, E. d. 2005. Research and Practice of Active Learning in Engineering Education. Amsterdam: Amsterdam University Press.
Padman, V., and Memon, N. 2002. "Design of a virtual laboratory for information assurance education and research," 2002 IEEE Workshop on Information Assurance and Security, Wesp Point, NY, p. 1555.
Paulsen, C., McDuffie, E., Newhouse, W., and Toth, P. 2012. "NICE: Creating a Cybersecurity Workforce and Aware Public," IEEE Security & Privacy (10:3), pp. 76-79.
Paulson, D. R., and Faust, J. L. 1998. "Active Learning For The College Classroom." Retrieved 01/12, 2019, from http://www.calstatela.edu/dept/chem/chem2/Active/main.htm
Peffers, K., Tuunanen, T., Gengler, C. E., Rossi, M., Hui, W., Virtanen, V., and Bragge, J. 2006. "The design science research process: a model for producing and presenting information systems research."
Ragan, T. 2013. "21st-century DevOps--an end to the 20th-century practice of writing static build and deploy scripts," Linux J. (2013:230), p. 5.
Rathod, N., and Surve, A. 2015. "Test orchestration a framework for Continuous Integration and Continuous deployment," Pervasive Computing (ICPC), 2015 International Conference on, pp. 1-5.
Ross, W., and Duke, E. 2017. "Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future," Commerce and H. Security (eds.). Washington, D.C.
Savery, J. R., and Duffy, T. M. 1995. "Problem Based Learning: An Instructional Model and Its Constructivist Framework," Educational Technology (35:5), pp. 31-38.
Schweitzer, D., Gibson, D., and Collins, M. 2009. "Active Learning in the Security Classroom," 42nd Hawaii International Conference on System Sciences (HICSS): IEEE.
Subrata Acharya, and Ryoo, J. 2010. "Standardization of Virtualization Efforts in Information Assurance Education for Intrusion Detection/Prevention Learning Modules " 14th Colloquium For Information Systems Security Education, Baltimore, MD, pp. 1-6.
Tam, M. 2000. Constructivism, Instructional Design, and Technology: Implications for Transforming Distance Learning.
Weiss, R., Mache, J., and Locasto, M. 2014. "EDURange: hands-on cybersecurity exercises in the cloud " J. Comput. Sci. Coll. (30:1), pp. 178-180.
Xu, L., Huang, D., and Tsai, W. 2014. "Cloud-Based Virtual Laboratory for Network Security Education," IEEE Transactions on Education (57:3), pp. 145-150.