Design for an Educational Cyber Range

Ryan Brunner
ryan.brunner@westpoint.edu
United States Military Academy
West Point, New York

Sang Keun Oh
sangkeun.oh@westpoint.edu
United States Military Academy
West Point, New York

Jesse Ramirez
jesse.ramirez@westpoint.edu
United States Military Academy
West Point, New York

Paul Houck
paul.houck@westpoint.edu
United States Military Academy
West Point, New York

Nathaniel Stickney
nathaniel.stickney@westpoint.edu
United States Military Academy
West Point, New York

Raymond Blaine
raymond.blaine@westpoint.edu
Cyber Research Center
West Point, New York

ABSTRACT

The "Cyber Range" concept arose as a method for organizations to provide realistic training in penetration testing and incident response. These ranges often utilize virtualization to reduce cost and allow for rapid reconfiguration. However, virtualization management software is often expensive or difficult to install. This paper presents a management application using open-source software with the intent of allowing educators to rapidly create virtual ranges at minimal cost.

CCS CONCEPTS

• **Security and privacy → Network security**; *Systems security*; Intrusion/anomaly detection and malware mitigation; Web application security.

KEYWORDS

cyber range, education, training, virtualization, software defined networking

ACM Reference Format:
Ryan Brunner, Sang Keun Oh, Jesse Ramirez, Paul Houck, Nathaniel Stickney, and Raymond Blaine. 2019. Design for an Educational Cyber Range. In *Hot Topics in the Science of Security Symposium (HotSoS), April 1–3, 2019, Nashville, TN, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3314058.3317727

1 INTRODUCTION

The need for effective computer security professionals has risen dramatically in the past few years[7]. Recent data leaks and breaches have demonstrated the need for organizations to take the security of their networks and systems seriously. Many have turned to teams of professionals to provide cyber security, penetration testing, and incident response services. Such teams can be extremely effective at reducing the impact of or preventing a breach all together. However, assembling, maintaining, and employing such a team requires a wide variety of skills and orchestration to be effective. This can only be accomplished with quality training and rehearsals in a realistic operational context.

The resources needed to train an effective information security team are significantly greater than the resources needed to train a single professional. An individual can train and practice in a local environment, such as a laptop computer, whereas a team needs a much more robust network in order to train in concert. Academia, government, and industry are increasingly turning to cyber ranges to fulfill this need[5]. Cyber ranges seek to provide high-fidelity simulations of realistic networks in order to present practical scenarios for teams. Providing this level of training requires significant resources, including compute hardware, management software, and administrator time, making them prohibitively costly for many organizations. Ranges may also be difficult to deploy because software designed to create and manage them tends to be either proprietary or difficult to setup. This work proposes a design for a cyber range framework which solves both the cost and complexity issues.

2 PURPOSE

The framework presented here seeks to provide users with a simple and easily extensible application to create and manage cyber ranges. For the purposes of this work, a cyber range is defined as an isolated network of virtual machines. Key to implementing this concept is containing traffic within the range in order to protect the security of external networks. Failure to do so could result in destructive tools being used against unintended targets. Furthermore, this project emphasizes the need for realistic target systems and network topologies in order to provide training which closely resembles scenarios that teams would face in the real world. A complete solution will allow users to create and manage target systems within the range, as well as the networks which connect those systems and the associated connections to external networks.

3 DESIGN

The application consists of three major components: a virtualization platform, a controller, and a graphical user interface. The current implementation uses Linux servers to host the virtual machines using the Libvirt API[3]. A REST API then serves as the controller[6]. This API layer provides a consistent interface to control the virtualization platform, allowing us to use any graphics framework for the user interface, so long as it can send and receive HTTP data. A web application is provided to act as the user interface, but other frontends could be used. Separating these components simplifies

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).
HotSoS, April 1–3, 2019, Nashville, TN, USA
© 2019 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-7147-6/19/04.
https://doi.org/10.1145/3314058.3317727

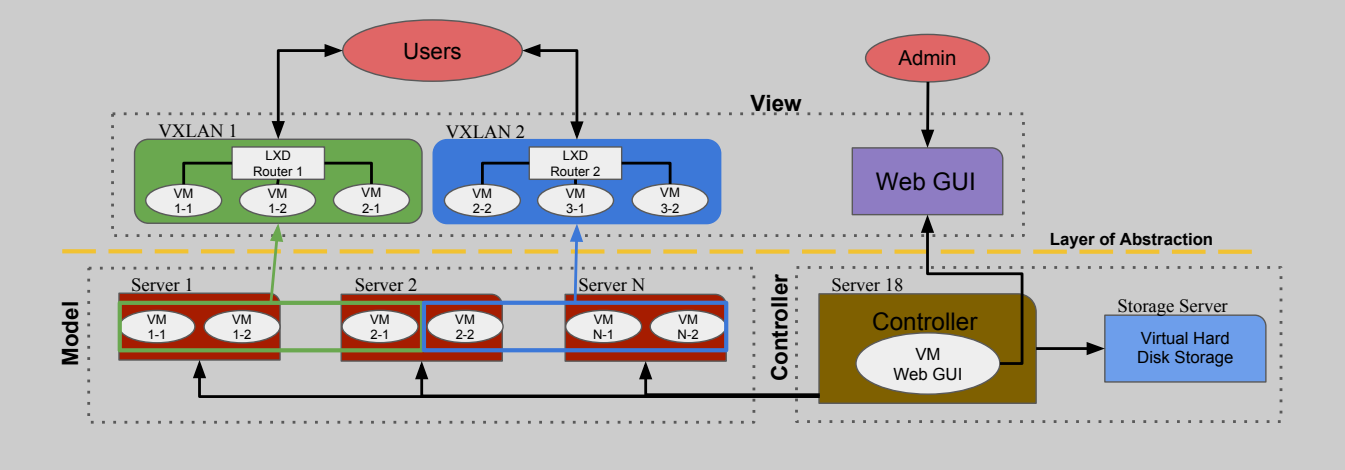


Figure 1: Major Components of Cyber Range

the construction of the application as the components only interact through a separate communication layer. It also allows us to replace individual components so long as they interact consistently.

3.1 Virtualization

Several virtualization backends were evaluated in the design of this application. The primary factors which contributed to the final choice were cost, ease of use, availability of documentation, and scriptability. Key factors are cost and ease of use, as the primary intent is to make this application cost effective and easy for the end user to manage. Commercial solutions such as ESXi[2] score well in many of these factors, but would prove to costly for many small organizations. Likewise, some open-source solutions such as OpenStack[1] and Proxmox[4] are either difficult to use or poorly documented. Libvirt was chosen for this application because it provides the best balance of these factors. Libvirt does not provide many of the high-level tools and management options that others provide, such as clustering and web management interfaces, but is open-source, has programming bindings in several languages, and is available on most Linux distributions. In choosing Libvirt, we also necessarily chose to design and implement a form of overlay networking in order to provide a full solution to the stated problem.

3.2 Networking

Overlay networking is vital to the function of a cyber range, since it allows for hosting more virtual machines than a single host can manage. Additionally, an overlay network allows for simultaneous hosting of separate networks so that multiple ranges with different purposes could be run at once. The chosen virtualization software, Libvirt, does not provide for overlay networking, which is a major barrier to the goals of this application. To overcome this problem, the authors chose the VxLAN protocol to implement overlay networks[8]. An example of the capabilities of VxLANs can be found in Figure 1. VxLANs allow us to leverage the flexibility of software defined networking without complicated management software. This does require a custom solution to manage the network, but the tools to do so are well supported and documented. The `iproute2` is one example of these tools and uses the VxLAN functionality of native Linux virtual switches. This method of creating overlay networks is transparent to the user and allows for greater customization than other software defined networking methods.

4 CONCLUSION

The key function of a cyber range is to provide an isolated network of target machines that allows information security teams to practice in a environment with a high degree of realism. The application presented in this work provides a minimal solution to easily create and manage virtual cyber ranges at low cost. This allows organizations to focus on training their teams rather than expending time, effort, and financial resources on range setup. The simple design and implementation of this concept will enable organizations to quickly deploy and tailor a cyber range to meet their needs. This allows an organization to provide cyber teams with situations which mirror the real-world environment where they will operate. The end state is that this environment allows more organizations to have access to the tools necessary to effectively train cyber teams.

REFERENCES

[1] [n. d.]. Build the future of Open Infrastructure. https://www.openstack.org/
[2] [n. d.]. ESXi | Bare Metal Hypervisor. https://www.vmware.com/products/esxi-and-esx.html
[3] [n. d.]. libvirt: The virtualization API. https://libvirt.org/index.html
[4] [n. d.]. Proxmox - powerful open-source server solutions. https://www.proxmox.com/en/
[5] 2018. Cyber Ranges. https://www.nist.gov/sites/default/files/documents/2018/02/13/cyber_ranges.pdf
[6] Roy Thomas Fielding. 2000. *Architectural styles and the design of network-based software architectures.* University of California, Irvine. http://dl.acm.org/citation.cfm?id=932295
[7] Paul Hernandez. 2018. New Data Show Demand for Cybersecurity Professionals Accelerating. https://www.nist.gov/news-events/news/2018/11/new-data-show-demand-cybersecurity-professionals-accelerating
[8] K. Duda P. Agarwal L. Kreeger T. Sridhar M. Bursell C. Wright M. Mahalingam, D. Dutt. 2014. Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks. https://www.rfc-editor.org/rfc/pdfrfc/rfc7348.txt.pdf