LearnFire: A Firewall Learning Tool for Undergraduate Cybersecurity Courses

Alicia Kirkland
Lewis & Clark College
Portland, OR 97219
akirkland@lclark.edu

Jens Mache
Lewis & Clark College
Portland, OR 97219
jmache@lclark.edu

***Abstract* - Cybersecurity is a fairly new topic in computer science. Firewalls are one of the most important elements in keeping a network secure. This paper describes the design, function, and goals of LearnFire, a collection of exercises for firewall education. LearnFire is designed to be used in the classroom as a hands-on learning tool, but can also be used by students independently. Each element of LearnFire aims to test varying levels of knowledge concerning firewalls. LearnFire is unique for three main reasons. First, it exists completely in the cloud, allowing students to access it inside and outside the classroom. Secondly, LearnFire tests the ability to build a firewall and to analyze an existing firewall for functionality and effectiveness. Lastly, and most importantly, LearnFire provides feedback for students to help further their learning and assess their progress.**

***Key Words*: security, firewalls, education, exercises**

I. Introduction

With the rise in cyberterrorism and hacktivism, companies are seeking people with cybersecurity experience more than ever. An article from Reuters reports that some of the largest companies in the United States are hiring cybersecurity experts to serve on their executive boards, which indicates increased concern with the threat network attacks pose today [1]. The demand for people with cybersecurity experience is on the rise, meaning that the demand for students who have experience building and analyzing firewalls is increasing. Firewalls are "network devices whose purpose is to enforce a security policy across its connections by allowing or denying traffic to pass into or out of the network" [2]. They play a huge role in cybersecurity. Therefore, it follows that in cybersecurity education, there should be tools aimed at teaching student how to properly build a new firewall and analyze an existing one.

Since class time is limited, exercises used in class must be efficient and useful. They should not take a considerable amount of time to set up and troubleshoot. Additionally, exercises must supplement the lesson, test students' ability to produce content, and check that students truly understand the meaning of what they have learned. Simply stated, good learning tools test students' ability to build and analyze, while providing feedback that students can use to assess their learning progress. LearnFire does exactly that while existing conveniently in the Amazon Web Services (AWS) cloud. LearnFire emerged as an alternative to two other firewall learning tools: DETERLab and FireSim [3, 4].

II. Related Work

In the Cybersecurity course at Lewis & Clark College, we used two exercises to practice firewall skills: a DETERLab scenario and a firewall simulation game called FireSim.

A. DETERLab

DETERLab is an environment in the cloud that provides virtual machines for students to perform experiments. Instructors must work with DETERLab to set their students up with accounts. After this, starting an experiment takes less than ten minutes on average. DETERLab provides reading material for students as an introduction to firewalls, specifically IPTables. This is important because the syntax for IPTables is complicated and can be confusing for students who have never worked with them.

The DETERLab scenario is a fairly simple lab exercise. The student acts as a security administrator for a company. The lab gives students a list of requirements for the firewall and the students create a firewall from scratch.

This scenario is a great first step in learning about firewall configuration. However, it lacks complexity. Students must simply build a firewall and submit it to their instructor. The lab instructions provide methods to test the firewall, but there is no feedback beyond that (besides instructor feedback). It does not test students' analysis skills. Setup time for this is minimal. Students must begin their experiment on DETERLab and log in to the virtual machines using an ssh client.

B. FireSim

FireSim is a competitive learning tool that requires students to build a firewall as protection against attacks from other students. Professor Ken Williams of North Carolina A&T State University developed FireSim using a Java applet and XML files. To use FireSim, instructors must download a group of files on a computer that acts as a web server. There is an additional computer that acts as the administrative computer that the instructor uses to add tasks over time. Each student operates his or her own computer.

The scenario lists a series of requirements that the students must respond to by building a firewall that allows and denies traffic according to the requirements. For example, the initial configuration of the firewall must allow domain name server access, access by the public to the student's website, and email from other email servers using SMTP. Students then attack each other's networks, gaining points when their attacks are successful and losing points when their network is attacked. Students update their firewall in response to successful attacks and new requirements designated by the administrator.

FireSim has an excellent concept. It provides a competitive environment for a classroom, which engages students differently than a lecture or lab. The goal of the game is easy to explain and understand. However, some of the tasks are a little tricky and vague Some of the tasks do not require a rule, but students do not know or understand this due to the minimal feedback provided by the game. Additionally, FireSim itself is buggy. Beyond that, the game could give more feedback and does not engage the students with what's happening under the hood. Students will understand how to write a rule to block access, but they might not understand what the rule means or why it blocks access.

III. LearnFire Scenarios

LearnFire is a collection of exercises for students to practice building and analyzing firewalls. It will be part of EDURange, a cloud based resource for hosting on-demand interactive cybersecurity scenarios [5]. LearnFire will have at least three scenarios, with more being developed over time and as new firewalls and methods emerge in the field. These scenarios test skills concerning various types of software and hardware firewalls. The initial scenarios focus on IPTables, Berkley Packet Filter (BPF) [6], and Palo Alto Networks.

Feedback is a very important feature in LearnFire. It allows students to further understand the topic at hand and gives them clear guidelines on where there are gaps in their knowledge and where they need to invest more time.

A. Scenario 1

The first scenario tests students' ability to analyze an existing firewall and create firewall rules. The student has access to two or more nodes in the cloud, represented by A, B, and C in Figure 1. Each node has its own set of firewalls (using IPTables and/or BPF), represented by A1, B1, and C1. The student must complete a series of tasks such as pinging one node from the other, sending a file, using SSH, and more. Students will have to edit, add, or delete rules in order to complete their tasks. They must record what they did to complete each task. This scenario only requires a network connection and a command line where a student can sign in to connect to the virtual machine. In terms of feedback, the scenario acknowledges completed tasks and gives hints when prompted by the user.

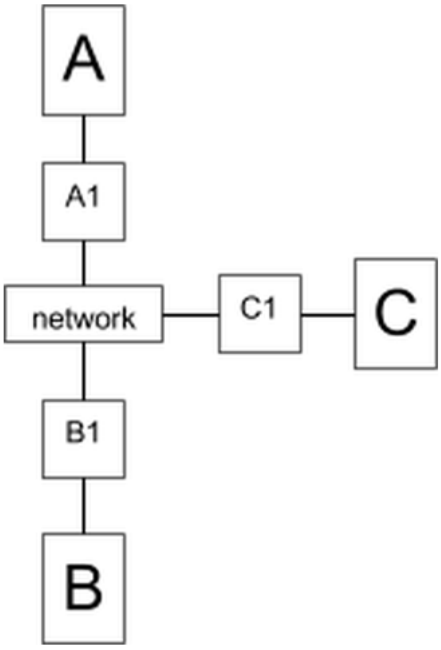

Figure 1: Conceptual Diagram of an example topology for Scenario 1

B. Scenario 2

Similar to FireSim, this scenario will provide a more competitive platform for students, represented as Alice and Bob in Figure 2. Each student builds their own firewall, represented by A1 and B1, to prevent their opponent from gaining access to their machine. The scoring agent will be live, constantly checking the command line and status of each virtual machine, and sending messages to each student to update them on the points they have won through penetrating their opponent's system and points they have lost due to their opponent succeeding in penetrating their system. The game can be timed or untimed, depending on the instructor or student preference. The scoring agent provides feedback by telling the students that they have gained or lost points and why that's happened.

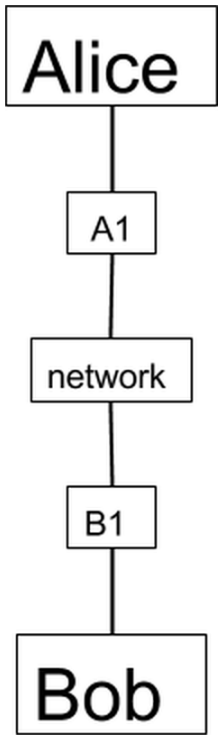

Figure 2: Conceptual Diagram of Scenario 2

C. Scenario 3

This scenario shifts the focus from software firewalls to hardware firewalls. Palo Alto Networks (PAN) worked with us to configure a virtual machine that uses their user interface to build a firewall for a network. PAN is a next-generation firewall [7]. Rather than filtering traffic based on ports and IP addresses, PAN allows the user to build a firewall that filters traffic using user

identification, content identification, and application identification. This new technology is more similar to what someone would experience in the professional world as the security administrator for a network.

Students will have access to three virtual machines: a management console, a machine inside the network, and a machine outside the network. The students will be able to interact with the management console to access the traffic rules and use the other machines to generate traffic. A question posed by the scenario might ask, "Which rule limits Alice's ability to send a Facebook message?" or the scenario might call for the student to perform a task and check the rules if the task fails. Students must analyze the existing firewall and think critically about the meaning of each rule. Feedback would appear in the form of telling the student whether their answer is correct and why or why not.

IV. Future Work

As this is currently in development, it has not yet been tested with students. The scenarios will be tested using students at Lewis & Clark College as well as other student volunteer groups in the Pacific Northwest from participating institutions.

V. Conclusion

LearnFire creates a learning environment in the cloud for students to develop firewall skills. The minimal setup time makes it an effective exercise for in class work and its cloud availability allows students to work from home. The feedback features engage students and allow them to build on their knowledge and push themselves to learn more. Overall, LearnFire is an excellent tool for educating students in order to fulfill the demand for cybersecurity experts.

VI. Acknowledgements

The National Science Foundation grant 1141314, the John S. Rogers Science Research Program of Lewis & Clark College, and the James F. and Marion L. Miller Foundation provided funding for this project. Special thanks goes to Richard Weiss.

VII. References

[1] Nadio Mamouni (2014, May 30). *U.S. companies seek cyber experts for top jobs, board seats* [Online]. Available: http://reuters.com

[2] Wm. A. Conklin and G. White. "Intrusion Detection Systems and Network Security" in *Principles of Computer Security: CompTIA Security+ and Beyond*, 3rd ed. Emeryville, CA: McGraw-Hill/Osborne, 2012, Ch. 13 pp. 334

[3] K. Williams. Firewall Simulation [Online]. Available: http://williams.comp.ncat.edu/FireSim/index.htm

[4] P. Peterson and P. Reiher. POSIX Permissions and Stateful Firewalls [Online]. Available: https://education.deterlab.net/file.php/12/PermissionsFirewalls_UCLA/Exercise.html

[5] S. Boesen, R. Weiss, J. Sullivan, M. Locasto, J. Mache, E. Nilsen, "EDURange: Meeting the Pedagogical Challenges of Student Participation in Cybertraining Environments", CSET Workshop, USENIX Security Symposium, 2014

[6] S. McCanne and V. Jacobson, "The BSD Packet Filter: A New Architecture for User-level Packet Capture," LBL, Berkeley, CA, Dec 1992

[7] J. Snyder. *What is a next-generation firewall?* [Online]. Available: http://networkworld.com