NETWORK FIREWALL VISUALIZATION IN THE CLASSROOM[*]

1st Lieutenant Justin Warner, 1st Lieutenant David Musielewicz, 1st Lieutenant G. Parks Masters, 1st Lieutenant Taylor Verett, 1st Lieutenant Robert Winchester and Dr. Steven Fulton
United States Air Force Academy

ABSTRACT

The implementation of network firewalls can be a difficult concept for students to grasp initially. Our Network Firewall Visualization tool, a capstone project created by our students, uses visualization (the graphical display of a simulation) to convey and teach network security and firewall configuration to students of all levels. This tool is intended to teach and reinforce key concepts including the use and purpose of a perimeter firewall, the use of separated subnets, the purposes behind packet filtering, and the shortcomings of a simple packet filter firewall. The expectation was that through the use of this tool students will gain a better understanding of the importance and use of network firewalls and their role in network security. This paper outlines the rationale behind the creation of the tool, how the tool is used in a classroom environment and demonstrates the improved understanding of the role of firewalls by students after using the tool in a guided classroom environment. The findings of this paper suggest a better student comprehension on written assessments following structured usage of this tool.

I. BACKGROUND

For years, our institution has taught a Computer Security/Information Warfare class as part of its computer science curriculum. The focus of this class is to teach students how to secure systems through understanding weaknesses inherent in computer systems and the vulnerabilities associated with networked computers. This class is part of the school's information security curriculum which is recognized by the National Security Agency and the Department of Homeland Security through its designation as a Center of Academic Excellence (CAE) in Information Assurance. The CAE designation is awarded based on an academic institution's ability to demonstrate the integration of a number of security topics within its curriculum [1].

[*] This paper is authored by an employee(s) of the United States Government and is in the public domain.

The Computer Security/Information Warfare class is taught annually and made up of primarily senior Computer Science majors. While, this class recently became a core requirement for all computer science majors, it also attracts other majors including basic science and system engineering students. The course is a mix of both lecture and hands-on laboratory sessions. This combination allows students to satisfy the need for theoretical education while permitting reinforcement of theory with tools and techniques on a practical basis. Such reinforcement helps to keep students interested while allowing them to see a more practical side of the theory being presented.

In the past, such hands-on reinforcement required complex lab configurations. In the case of networking topics, these environments may require isolated configurations in which students can create and configure networking environments [2], complex virtualization environments in which students create and modify virtual network environments [3] or animation of presentations using computer based flash environments [4]. Furthermore, we have discovered that differing student skill levels make hands-on labs difficult as some students grasp theoretical computer science topics more easily than others and have more experience with hardware and operating systems. In an attempt to meet the educational needs of all students, our department has turned to visualization tools to present such topics instead of attempting to bring a room full of students' skills to the same level prior to tackling a difficult subject in a complex lab environment.

II. CLASSROOM VISUALIZATION TOOLS

Hands-on labs are seen as an effective way to teach students real world vulnerability, attacks, and tools in information warfare [5]. Such hands-on labs in the information warfare arena come with their own problems including the previously mentioned range of student knowledge and the difficulty simplifying these topics without reducing the topic to a simple script kiddy tool which doesn't reinforce underlying theory [6]. One solution is to use visualization tools which permit the teaching of a topic through simulation in a self contained environment. Such visualization tools can be an effective means for reinforcing complex concepts and teaching challenging material. We've found that single purpose tools can be used in several different ways such as teacher demonstration, student labs, and homework exercises as well across different student skill levels. Each use might bring about a different level of understanding for the student from general comprehension to deep learning (a change which carries beyond the end of the training effort) [7]. A visualization tool should, in an ideal situation, be enjoyable to use as well as easy to understand so that students can actively learn the concepts while applying the concept to the real world [8]. Connections between tool and concept must be subtle yet meaningful and easy to understand so central ideas can be taught while keeping the student's focus. Hands-on interaction with the visualization tool along with realistic scenarios permits students to interrelate the subject with a concrete experience. For the majority of students, this makes learning complicated concepts easier and more important [9].

III. THE NETWORK FIREWALL VISUALIZATION TOOL

Five senior students recently created the Network Firewall Visualization Tool under the mentorship of a faculty member during their capstone course. This capstone course is taught during two sequential terms in which students work on projects identified by either faculty members or industry representatives. The goal of the capstone course is to permit teams of students to perform real world system engineering functions including formal design review meetings, schedules with strict milestones and detailed system analysis with the customer being the organization or person who has requested the project.

The need for the Network Firewall Visualization Tool was identified by CS department faculty members who teach network topics to various class levels. The goal of the tool is to give students the opportunity to experiment with creating firewall rules to identify and stop network attacks. Accomplishing this task using actual firewall equipment would be expensive and difficult to maintain and monitor in a lab environment.

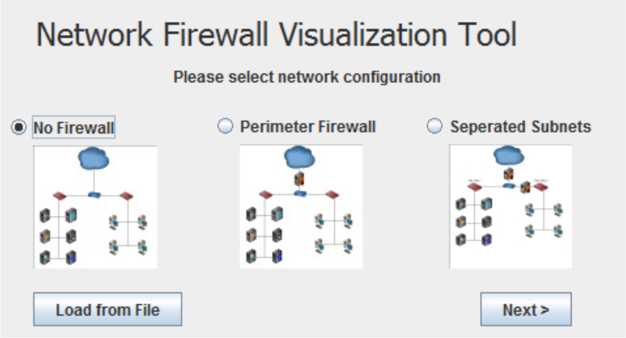
The Network Firewall Visualization Tool is a Java based program designed to run on individual laptops. At our institution, students are required to purchase laptops as freshmen and to bring them to their classrooms to perform tasks associated with the individual classes such as note taking and programming.

The Network Firewall Visualization Tool represents three distinct networking environments: a network with no firewall, a network with a single firewall, and a network with two different firewall configurations. The tool is further separated into several major components:

Network Selection
Traffic Definition
Simulation Control
Simulation Report
Simulation
Rule Creation
User Help

With the exception of the network layout, each component can be dynamically modified at any time during the scenario and the simulation will automatically update its course of action. For example, after defining traffic type and beginning the simulation, rules may be changed or new attacks may be added. The simulation will update automatically to reflect these changes. Furthermore, the current network setup including network selection, traffic, and rules can be saved to a file at any time for use in a later demonstration.

A screenshot of the network selection dialog is shown in Figure 1: Network Selection Dialog Box. By default, our tool provides three standard network layouts common in traditional network security: no firewall, perimeter firewall, and a two firewall setup with a DMZ. As seen in Figure 1, the user has the ability to select which layout they would like to use or to load prebuilt scenarios from a file. This allows faculty members to create scenarios which can be loaded shared with the class. Additionally, students who have problems understanding a given scenario can save that scenario and share it with the instructor to allow the instructor to provide an analysis and feedback of the student's specific situation.



Network Firewall Visualization Tool

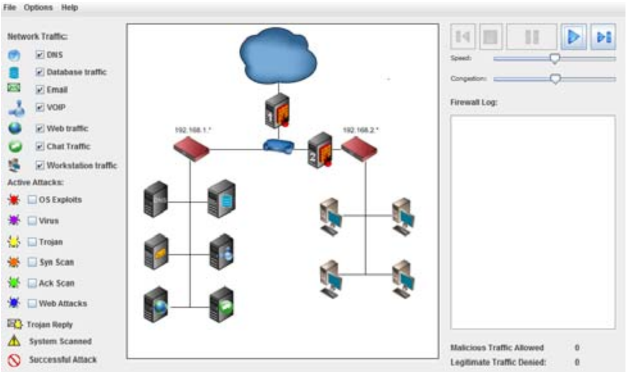
Please select network configuration

● No Firewall ○ Perimeter Firewall ○ Seperated Subnets

Figure 1: Network Selection Dialog Box

After selecting a network or loading a scenario, the user enters the primary simulation screen as seen in Figure 2 – Main Simulation Window. The user may select options on the left to define the traffic present in a given scenario. Options allow enabling all of the represented services such as chat traffic, VOIP traffic, or DNS queries. When traffic is generated, it is visually reflected in the tool.

Some common attacks were included to test overarching concepts such as trojans (which exploit systems by removing information) or viruses (which propagate traffic which is hard to stop with packet filtering). As in real life scenarios, some of the attacks can not be stopped by a firewall, while others may be more easily controlled in such firewall scenarios.



Network Traffic:
☑ DNS
☑ Database traffic
☑ Email
☑ VOIP
☑ Web traffic
☑ Chat Traffic
☑ Workstation traffic

Active Attacks:
□ OS Exploits
□ Virus
□ Trojan
□ Syn Scan
□ Ack Scan
□ Web Attacks

Trojan Reply
System Scanned
Successful Attack

Speed:
Congestion:

Firewall Log:

Malicious Traffic Allowed 0
Legitimate Traffic Denied: 0

Figure 2: Main Simulation Window

The user can control the simulation using the buttons and slide bars in the upper right hand corner of the main window. These controls allow users to start, stop, pause or navigate through the scenario using buttons similar to the common DVD player (See Figure 2).

During simulation usage, students can measure their success with the firewall or debug a rule set using the log window on the right side of the main screen. This log screen will display blocked packets by source, destination, port and protocol. The counters at the bottom right indicate the number of malicious packets allowed through the firewall and the number of legitimate packets that were blocked. Ideally, a rule set would minimize both of these numbers. The goal of this tracking is to allow students to grasp the concept of the balance between security and usability while demonstrating that it is possible to secure a system to the point that it denies both legitimate and malicious traffic.

Figure 3: Firewall Simulation with Active Traffic illustrates the active usage of the system. Network packets are listed in the legend on the left as symbols (an envelope for e-mail packet, disk platter for database traffic, and so on). As traffic flows along the network, the symbol associated with a given packet moves from the Internet cloud to a given computer, or between computers depending on the type of traffic. For example, mail traffic may flow into the system from the Internet, or from a workstation to the mail server. As active attacks take place, small color coded 'bugs' travel across the network

to different machines as shown in Figure 4: Tool Icon Breakdown. The color coded symbols identify the type of attack being perpetrated against the network (i.e. red bugs symbolize an operating system exploit, etc.). Successful infection of a machine is identified through the use of the 'international no' symbol. Furthermore, once a machine is infected, that infection can spread to other workstations or servers, just as in a real life situation. By following traffic down the network, it is possible for the user to identify where the traffic flows and which systems are vulnerable to attack. As packets continue through the system, firewall logs are kept similar logs kept in active firewall systems. These logs are scrollable through the Firewall Log window.

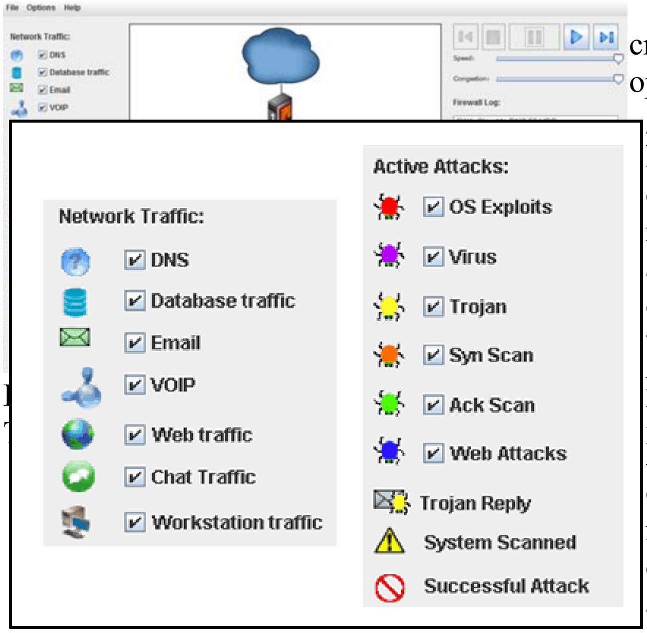


Figure 4: Tool Icon Breakdown

Users configure the tool by creating rules. To do so, the user opens up the firewall rules dialog for a given firewall as seen in Figure 5: Firewall Rule Dialog. Within this dialog, there are two boxes on the right which contain activated rules and inactive rules. New rules are created by first clicking on the "clear" button and inputting all of the required information (Name, Source IP, Source Port, Destination IP, Destination Port and Protocol). Once created, a user can move individual rules to the inactive side for debugging without having to delete and recreate the rule for later analysis. Rules are applied in the order in which they are placed in the active box. To simplify the configuration of the rules, users can use the drop-down boxes to select which service they desire for the source or destination and to use the auto-complete feature for the IP Address and Port information. The user can then save the rule by selecting the "save rule" button. If a rule needs to be modified or viewed, the user can click on the desired rule and the information will be updated in the correct fields. Finally, the user can make the firewall stateful by checking that option to prevent ACK Scans from passing through the firewall by reviewing the data within the packets to see if they are harmful to the network.

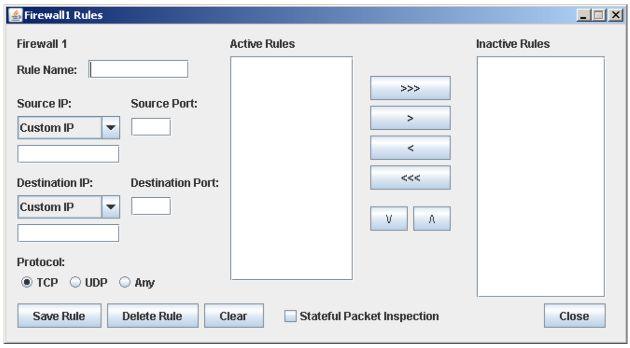
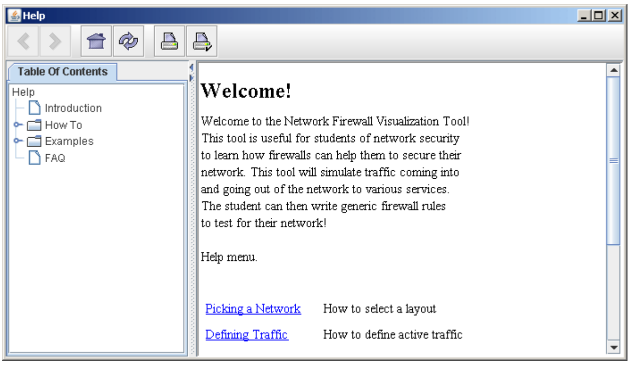


Figure 5: Firewall Rule Dialog

For help with all of these functions and concepts, the user can refer to the help documentation as illustrated in Figure 6: Help Dialog. The help pages are laid out to assist the user through each step of creating a scenario. Should the user want to skip to a specific area of the Help function, they can use the Table of Contents provided on the left hand side of the window. This help function was designed to mimic standard Microsoft Windows help functions.



Welcome!

Welcome to the Network Firewall Visualization Tool!
This tool is useful for students of network security
to learn how firewalls can help them to secure their
network. This tool will simulate traffic coming into
and going out of the network to various services.
The student can then write generic firewall rules
to test for their network!

Help menu.

Picking a Network How to select a layout

Defining Traffic How to define active traffic

Figure 6: Help Dialog

IV. TOOL USAGE

Our experience using visualization tools in the classroom suggests that students benefit from a formal guided path through the program. We have accomplished this by using exercises which not only guide the student through the use of the tools but also ask specific questions that force the student to draw conclusions based not only on what the tool shows them but their interaction with it. For example, in one exercise, a student is asked to create a rule with the following format:

Rule Name: DNS Rule
Source IP: DNS, Source Port: 53
Destination IP: Any, Destination port *
Protocol: Any.

Once the rule has been created, the student will begin the scenario by clicking the play button. As the traffic begins traversing through the simulation, students are then asked questions such as:

- What traffic now flows through the firewall?
- Would you claim your rule is now sufficient to allow traffic to flow for a typical network? Why or why not?
- Do any of the active attacks now work against machines behind the firewall?

Without such formal guidance on the tool usage, we suspect the students will focus on the game-like aspect of the tool instead of focusing on understanding the rationale behind an attack being presented.

Such specific questioning of students also provides the opportunity to assess student understanding of a given scenario. At the end of the lab session, students submit answers to the formal questions for assessment by instructors. Such assessments allow instructors to understand exactly how well students are grasping a given topics.

By focusing on multiple attack types such as SYN, web attack, and ACK, the student is forced to ascertain why a given rule would stop one type of attack while permitting others. An example of this would be the SYN attack. In a SYN or TCP SYN Flood attack, a series of valid requests for a service is generated yet no connection to that service is created [10]. This would be something that is not typically solved using a firewall solution but instead by ensuring that the computer does not permit substantial hanging service requests. The simulation actually permits these SYN attacks to go through the firewall regardless of what students do to restrict this. By treating these attacks as they would be in the wild, students are forced to understand the details of the attack and recognize why it successfully bypassed the rule set to reach machines behind the firewall.

The additional flexibility of saving and reloading scenarios allows instructors to create a given rule set and share it with the students. Our experience has been that this feature allows students to explore more complex rule sets than would normally be created during the class itself.

V. CLASSROOM USAGE

The firewall visualization tool was used in two different offerings of our Information Warfare class. Prior to the introduction of this tool, the topic of firewalls was strictly a lecture lesson in which students were asked to identify the results of rules associated with a given topic. There was no firewall lab exercise associated with the material.

In preparation for using the firewall tool, students participated in a 20 minute lecture-based overview of the role of firewalls in computer/network security followed by a demonstration of the visualization tool. Students were given the rest of the period to work with the guided exercise described previously. The instructor's role in this scenario was to ensure that students were completing the exercise and that they fully understood the scenario.

Initially, students followed a number of guided scenarios in which they were asked to configure the tool for a given situation. For instance, they were asked to create a Perimeter Firewall which has DNS, Email and VOIP traffic and is attacked by both Viruses and Trojans. They are asked questions such as: Can you create a series of firewall rules in which malicious traffic never enters your network? or What rules did you create to do so? Additionally, students were asked to load an instructor created scenario and identify weaknesses in the firewall configuration. The exercises were followed up by a series of questions to assess the understanding of the firewall topics by the students.

Following the exercise, a written survey was given to the students in an attempt to ascertain the value of the tool for the students.

When asked about the usefulness of the tool following the exercise, 82% of the students responded that the tool was very useful in clarifying topics provided in the lecture compared with 14% who felt that this tool did not have additional benefit to the lecture alone. When asked about the complexity of the tool, 95% of the students felt that the tool was simple to use. 83 percent of the students found the tool to be helpful in clarifying complex topics.

While the use of a firewall is discussed in a single lesson, several prior lessons presented topics about related network vulnerabilities such as viruses, Distributed Denial of Services, and SYN Flood attacks. The guided lab exercise exploited this tool to re-enforce these topics, too. Such high level positive student response suggests that the tool helped to bring together these various concepts in a single lesson.

VI. CONCLUSIONS

The overall results following the use of the tool in the classroom setting was positive. Students found the tool informative and interesting to use. Written assessments relating to the use of firewalls also demonstrated positive learning efforts with an average of 84% on questions relating to the purpose and use of firewalls on the course assessment.

The structured usage of the tool coupled with the guided scenarios helped students to understand both how to use the tool as well as the strengths and weaknesses of firewalls. Open-ended questions in the scenario required students not only to understand how to create firewall configurations but to understand the role of firewalls in securing a network. The high number of positive responses to the tool suggests that the students accepted the tool as an integrated course learning experience.

The written survey allowed the students to provide some general comments regarding the tool. 45% of the comments on the tool were positive and no negative comments offered. What was interesting was that the remaining 55% of the comments offered suggestions on ways that the tool could be modified to bring about additional learning beyond the current design such as adding definitions for attacks, allowing increased congestion of a given attack would have helped or requesting a final statics page. The number of unsolicited student comments focusing on new features suggests that students see additional value in the tool beyond its initial design and saw value in the use of the tool in other network related classes.

VII. FUTURE PLANS

The tool was designed with a requirement of expandability. Faculty interest in the tool includes the possibility of supporting IPSec implementation between services, drag and drop network design, expanded types of traffic or attacks, and the ability to put the tool in an advanced mode for a more in depth teaching of how firewall design works.

Current plans include the use of this tool in a beginning computer science survey course to help simplify the use of firewalls as a security tool.

VIII. REFERENCES

[1] Schweitzer, D., Humphries, J., and Baird, L., Meeting the criteria for a Center of Academic Excellence (CAE) in information assurance education. *Journal of Computing Sciences in Colleges,* 2006. 22(1): 160.

[2] Romney, G. and Stevenson, B. An isolated, multi-platform network sandbox for teaching IT security system engineers, in *Proceedings of the 5th conference on Information technology education*: 2004: 19-23.

[3] Begnum, K., Sechrest, J., and Jenkins, S., Getting more from your virtual machine. *Journal of Computing Sciences in Colleges*, 2006. 22(2): 73.

[4] Bergstrom, L., Grahn, K., Karlstrom, K., Pulkkis, G., and Astrom, P., Teaching network security in a virtual learning environment. *Journal of Information Technology Education*, 2004. 3: 189-217.

[5] Yurcik, W. and Doss, D. Different approaches in the teaching of information systems security, in *Proceedings of the Information Systems Education Conference: 2001*.

[6] Schweitzer, D. and Fulton, S., "A Hybrid Approach to Teaching Information Warfare " in *5th International Conference on Information Warfare and Security 2010*. Dayton, OH. pp.

[7] Marton, F. and Saljo, R., On qualitative differences in learning: 1--Outcome and process. *British Journal of Educational Psychology*, 1976.

[8] Schweitzer, D. and Brown, W., Interactive visualization for the active learning classroom. *ACM SIGCSE Bulletin*, 2007. 39(1): 212.

[9] Schweitzer, D., Collins, M., and Baird, L. AVisual Approach to Teaching Formal Access Models in Security, in *11th Colloquium for Information Systems Security Education*.

[10] Stallings, W. and Brown, L., *Computer security: principles and practice*. 2008, Pearson Prentice Hall.