Midterm Report
for
"Scarlet Shield"

Capstone Design in Computer Systems
14:332:438

Team 2:

Jeff Adler
Eric Cuiffo
Parth Desai
Jeff Rabinowitz
Val Red

April 1, 2014

Contents

1 Proposal: Network Threat Analysis and Deterrence Automation

1.1 Motivation

One of the major issues confronting all computer networks today is cyber security; the goal of our Network Threat Analysis and Deterrence Automation capstone is to build an adaptive security system for large-scale switch networks to adapt and thwart attempts of exploitation and intrusion by analyzing TCP/IP packets and deploying a flexible response (such as the restriction of traffic via iptables or outright blocking the origin of offending packets) based on perceived threats over network. Penetration methods and exploitable vulnerabilities are evolving at an alarming rate. Increasingly dangerous practices such as the "Advanced Persistent Threat" (APT), a long-term network attack utilizing a plethora of effective methods to break into a system over a prolonged period of time, are becoming an increasingly intimidating issue confronting enterprise networks. Our threat analysis system will be a proof-of-concept for a stronger, more cooperative network security environment. Our intention is to start small and build a simple computing operating system that may be placed on a management role over a switch network that can preventively detect and deter brute force dictionary attacks, one of the easiest but most expensive attacks that can be utilized against a network. From there, we will expand our system to actively analyze, detect, and deter more sophisticated attacks (such as distributed denial of service attacks) by employing distributed computing practices to parallelize TCP/IP threat analysis and corresponding system policy changes to deter such attacks before they successfully penetrate a network. *There is a popular misconception that network attacks can only be deterred after successful intrusion; we would like to challenge that misconception with our Network Threat Analysis and Deterrence Automation capstone.*

Sources of Domain Knowledge

- *Val A. Red* is a system administrator for Engineering Computing Services and has experience with employing automation and network policy/iptables to administrate networks.
- *Eric Cuiffo*, *Parth Desai*, and *Val A. Red* have programmed a multithreaded SSH attack and successfully found a counter to it that can be easily implemented in any system.
- Professor Parashar coauthored "Cooperative Mechanism Against DDoS Attacks," which addresses a very specific type of attack and applies a process similar to what we would like to achieve on a large scale for a large number of known attack methods.

1.2 Abstract

With the advent of increasingly potent methods employed against cyber security such as GPU-based penetration attempts and the Advanced Persistent Threat (APT), there is an increasing need for network administrators to be cognizant of deploying, automating, and maintaining robust systems for managing their switches and network traffic. Due to the increasing volume and value of data being transferred over online networks, we intend to design and develop a system to reliably secure large networks from the switch-level with a deployable Linux kernel existing solely to monitor and manage a switch network, applying strict, sophisticated tools and programs (iptables, etc.) to adaptively and effectively prevent, deter, and thwart network attacks and penetration attempts

Deliverables

1. Documentation on the following:
    a) Set-up of the customized Linux kernel, describing how to replicate our system. (Including system requirements, sources and dependencies, etc.)
    b) Supplementary, custom packaged programs to enhance and automate traffic sniffing and group policy/access over ports/protocols depending on volume and potential threat of incoming TCP/IP packets.
2. A **live** web-facing server hosted by Engineering Computing Services (ECS) utilizing our custom defense system with common open ports (80 for HTTP, 22 for SSH, etc.) for testing and demonstration of the robustness of our system.

Goals

1. Prepare customized Linux kernel with customized, optimized iptables flexibility for network defense.
2. Utilize parallelized TCP/IP analysis to detect common network attacks.
3. Automate network access policy/permissions based on threat analysis.
4. Deter attacks before they succeed utilizing parallelized analysis and automated system responses.

Logistics

The automation aspects of our proposed capstone may be of great interest to Juniper Networks, who suggested a capstone very similar to what we propose with regards to the flexible changing of network policies based on different scenarios.

1.3 Anticipated Technical Challenges and Risks

1. Automating network traffic sniffing (interpreting TCP/IP packets) would be expensive and one of the most difficult aspects of our project to apply and has the risk of false positives. We will need to be very careful writing and employing programs that operate at this level.

2. If our proposed system is somehow compromised, it would essentially put an entire network at risk. Well need to ensure our system is robust and not readily accessible (employ a second access layer, such as restricting SSH access to the system to the internal network, etc.) to reinforce the security of the actual system.

3. There are countless kinds of attacks and every day there are more and more vulnerabilities and software updates to compete against such vulnerabilities, so we need to very early define which attacks well address with our system first that would be reasonable for the duration of semester and how we will approach sustainability over the long term.

1.4 Web Page

Our web page is currently hosted via Drupal at http://scarletshield.rutgers.edu.

1.5 Final Remarks

Overall, our proposed capstone would serve as a proof-of-concept for utilizing customized, robust operating systems to enhance switch and network management. Ideally, the combination of our choice and employment of various tools and self-authored programs in addition to the customized kernel should definitely contribute some insight for how network admins can flexibly apply their technical proficiency to keep their networks safe.