Network Security

Develop a tool that can protect a system from hacking

Project Proposal

ZAOXING LIU **CHANG LIU**

zaoxing@jhu.edu **chang.liu@jhu.edu**

We are sure that this work is not part of the project for another course.

Mar. 2, 2012

A. Background of the Problem

The Coordination Centre of the Computer Emergency Response Team at Carnegie-Mellon University has recorded a doubling of both software vulnerabilities and reported security incidents every year since 1999. Since the rates of intrusions and security incidents have increased dramatically in the last few years, there is an increasing demand for Intrusion Detection System for a network or system administrator to monitor and maintain the security of the network. In addition, the IDS system should not only be able to detect the malicious attempt from the attacker, but should also be able to prevent such attacks.

An Intrusion Detection and Prevention System (IDPS) is a software application that monitors the malicious networks and/or system activities or policy violations, furthermore, the application will log the said activities, attempt to block/stop activity, and report activity. Our goal in this project is to develop an Intrusion Detection and Prevention System that could monitor and handle some well-known malicious activities in the real network environment.

B. Citation of the Papers

[1] Rangadurai Karthick R., Hattiwale, Vipul P., Ravindran Balaraman, Adaptive Network Intrusion Detection System using a Hybrid Approach, 978-1-4673-0298-2/12/$31.00 c 2012 IEEE.

[2] Man Zhao, Jing Zhai, and Zhouqian He, Intrusion Detection System Based on Support Vector Machine Active Learning and Data Fusion, ISICA 2010, LNCS 6382, pp. 272–279, 2010.

[3] David J. Day, Benjamin M. Burns, A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engines, ISBN: 978-1-61208-116-8, IARIA, 2011.

In paper [1] and [2], we find that the hybrid mechanism on *Anomaly based detection* and *signature based detection* is more effective than the sole technology. And in paper [2], we will implement the new features of network data analysis and absorb the advantage of data fusion.

C. Description of the project

General Description:
Our project goal is to develop an integrated tool that could recognize and analyze unexpected accesses to a network. It is a feature rich Network Intrusion Detection and Protection System combining the modified snort platform and our Independent Design on front end. Our tool should have the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks. At the same time, the tool can produce some analysis charts and graphics to present the network traffic and network attacks, such as SYN Floods, DNS Spoofing attacks and buffer overflow.

Based on the Snort open-source platform, we will implement a new UI friendly system, which includes excellent snort rules and new alerting mechanism. This system mainly contains two modes:
The Sniffer Mode: In this mode, the system will detect the unexpected TCP, IP, UDP and ICMP packets and record them.

The IDPS Mode: This mode is based on the rules of snort and implement some basic monitoring and preventing functions.

Detailed Features

- METRICS & REPORTS

  This system brings existing SNORT's network security monitoring data to life with a suite of beautiful, relevant, and most importantly, actionable metrics. Meanwhile, this tool can share data like network-sensor activity comparisons or our most active signatures directly with our constituents with daily, weekly, monthly, and PDF reports.

- FULL PACKET

  Unlike most network security monitoring applications, this system integrates with new and existing OpenFPC, Solera DS Appliances, and Solera's DeepSee installations to give analysts full packet and session data.

- CLASSIFICATIONS

  With a simple keystroke or a mouse click, the analysts of this system can quickly classify an event into one of the many preconfigured classifications or into custom classifications relevant to an organization. Totally, we use classifications to organize events into helpful categories for follow-up investigations or for tuning the alert rule-sets.

- CUSTOM SETTINGS

  While this system is designed to work out of the box, it can add custom severities or classifications, manage email notifications, and even extend functionality with third party products.

Division of the work

Zaoxing Liu: mainly responsible for the analysis of Intrusion Detection mechanism on the original snort platform and the implementation of the monitoring and alerting functions on web-based front end.

Chang Liu: mainly responsible for the analysis on the network attacks and the implementation of new rules on snort environment.

Also, we will create a demo that can demonstrate the whole process of attacking, monitoring, alerting and prevention.

D. Description of the deliverables

The deliverables will be a software application that could detect and measure the risks on the network traffic based on the automatic analysis of snort platform.

The final deliverable should consist of the lower Intrusion Detection System platform (basic snort) and the user-friendly web based front-end with plentiful features on this platform.

E. Description of approach to produce deliverables

We plan to develop our program in a phase manner, for the first phase we want develop some basic functions/modules that could be easier to implement with simple output. For instance, the phase one product should be able to detect the Denial of Service attack and output/log the attacker's IP address. The goal of phase 1 is to make our application basically functional, more features will be added to the program in the phase 2.

In phase 2, while we becoming more and more familiar with the procedure and techniques to detect some well-known network intrusion activities and the methods to prevent them, we will start to add more features that could detect and analyze some more complex intrusion attempts like ARP attack or DNS Spoofing attacks. In addition, we will polish the products from both phase 1 and phase 2, all the output from each module/function will be in report format along with graphical display that will be easy for system/network administrators who have no experience in security to read and understand.

For phase 3, we will test all the modules/functions we developed during the phase 1 and phase 2, fix any bugs we may find during the test.

F. What will be novel/new in your project as compared to the chosen paper(s)? Describe the differences clearly

Nowadays, the alerting and analysis mechanism on snort cannot meet the new requirements of network security. Although the technology of *signature-based detection* on snort is still widely used, the original technology of the SNORT looks out of date now. In my opinion, the original data of network traffic and unauthorized network access from the SNORT is not what the users really need today. Actually, they need a system that can directly and clearly provide them the intelligent attacking monitoring and analysis functions. Thus, we will add a new feature rich web-based front end into the original snort platform and implement the higher-level functions of monitoring, alerting, analysis and prevention that can help the users protect their servers from attacking.

Besides, according to the paper [1] [3], the *Anomaly based detection* has its own advantages while the SNORT's major technology is *signature-based detection*. We will try to implement more features on *Anomaly based detection* and increase the efficiency of network detection.

G. Required Resources

- The snort open source platform for Intrusion Detection System
- Ruby and Rails
- Image Magick

- OpenSSH
- Ubuntu 11.10