1 Introduction

Whether an organisation's network connects to the Internet or not, it is exposed to security threats. Malicious activity can originate both internally and externally. As the network grows it will play host to numerous bugs and security loopholes that can be unheard of - but known to intruders. Organisations recognizing the value of good security policy will define what is and what is not allowed in terms of network and Internet access.

There are three integral parts to security technologies. One part consists of preventive measures: dial-back modems, smart cards, firewalls and all the technologies supposed to keep intruders or hackers out of your network. The second part comprises of assessment technologies, such as Satan and all the other scanning tools, that allow you to see your security flaws before the hackers see it. The third part involves intrusion detection techniques: ways to verify that, in fact, something has gone wrong with your security. Therefore, to protect an organisation completely, it is necessary to include the implementation of intrusion detection systems as a line of defense.

1.1 Intrusion Detection Systems

From a dictionary's perspective, 'intrusion' means to enter to another's property without right or permission. The word 'detection', on the other hand, denotes to discover or to determine existence of something. So together, the words 'intrusion detection' would mean discovering unauthorized entry to another's property.

In this research, intrusion detection systems, is addressed in the context of computer security where an IDS entails computing-related implications and does more

than merely discovering unauthorized entries. In a more technical approach, intrusion detection can mean audit trail processing, firewall filtering and logging, router-based access list usage, or even telephony-based toll, depending on the computing application.

In [Amoroso 1999], intrusion detection is defined as "the *process* of *identifying* and *responding* to *malicious activity* targeted at *computing and networking resources*." An entire category of software exists in the form of intrusion detection systems. These intrusion detection systems can typically be divided into two main types, network-based or host-based. Network-based IDSs look for attacks in the network traffic while host-based IDSs look for attacks in log files. Although recent advances in technology has given birth to commercially-driven hybrid IDSs that incorporate both network-based and host-based IDS technologies, they remain the more expensive solutions.

1.2 Evaluations of Intrusion Detection Systems

There has been a handful of evaluations performed on intrusion detection systems. Those cited in this dissertation are: one from NSS Group [NSS Group 2001], and two from the MIT (Massachusetts Institute of Technology) Lincoln Laboratory, under Defense Advanced Research Projects Agency (DARPA) sponsorship – the 1998 DARPA-LL evaluations and the 1999 DARPA-LL evaluations [Lippmann 2000, Lippmann 2000a]. The evaluations mainly involve the construction of a test bed, the generation of background traffic and test attacks, and finally the compilation and analysis of the results of the testing.

1.3 The Objectives and Benefits of Evaluating Intrusion Detection Systems

In general, the objectives of evaluating intrusion detections systems are mainly to provide unbiased measurement of current performance levels in intrusion detection system technologies and to drive iterative improvements in the systems evaluated by revealing their strength and weaknesses. The uncovering of strengths and weaknesses greatly helps researchers to focus on eliminating weaknesses. As a result, evaluating intrusion detection systems is essentially beneficial because it helps to focus effort, document existing technologies and guide further research.

1.4 Research Objectives and Contributions

This research has 3 main objectives that embody its contributions. They are as follows:

- To provide a method of how a one-person study can perform a thorough evaluation process on intrusion detection systems using publicly available test data sets and intrusion detection systems. IDS evaluations are normally infrastructurally complex and require the involvement of many researchers and participants. This research simplifies the evaluation method and makes it feasible for a one-person research to complete it within a reasonable amount of time.
- To provide a performance evaluation for four configurations of the selected IDS, Snort, by testing them against a variety of attacks and background traffic. Based on the test results, the detection rates for each configuration in every attack category are

calculated. The four different configurations are then conferred their respective performance ranking according to their detection rates.

- To uncover the weaknesses of previous evaluations after the experience of IDS testing and evaluating is garnered. From understanding past weaknesses, lessons can be learned in order to improve future evaluations of intrusion detection systems.

1.5 Research Methodology

This research focuses on evaluating intrusion detection systems. The testing and evaluation process involves the following steps:

1. Constructing a test environment. The test environment consists of the test machine, test data, the operating system on the test machine, Snort (the IDS to be tested), SnortSnarf (the utility that parses Snort's alerts) and the test results forms.
2. Implementing the tests. The implementation of the tests consisted of configuring Snort and running the test data sets through the four configurations of Snort. This is presented at length in chapter 5.
3. Gathering the results of the tests. Upon completion of a test run, the resulting alerts file is processed and put into an HTML report format by SnortSnarf. The results in this HTML report is then manually transferred to the corresponding results forms and the detection rates for the respective configurations are calculated.
4. Evaluating the IDSs based on test results. In this final step, the four Snort configurations are evaluated and conferred their performance ranking based on their respective detection rates. The performance of each configuration and the reasons

why certain attacks were undetected are also discussed. This is covered at length in chapter 7.

1.6 Research Scope

Four configurations of the chosen IDS tool, Snort, were tested against four attack-filled test data sets. The main reason for exclusively testing on snort, from which its different configurations are derived, is because it comes with a utility called SnortSnarf that parses the alerts from the alerts file.

The four configurations of Snort used in the testing were:

- Configuration 1 - Snort 1.7 Full
- Configuration 2 - Snort 1.7 Custom
- Configuration 3 - Snort 1.8.3 Full
- Configuration 4 - Snort 1.8.3 Custom

The four test data sets used (taken from: http://www.ll.mit.edu/IST/ideval/) for the testing was run through each of the above configurations. The test data sets are presented below:

- Test Data Set 1 – 1998 Learning Data Week 6
- Test Data Set 2 – 1998 Learning Data Week 7
- Test Data Set 3 – 1999 Test Data Week 1
- Test Data Set 4 – 1999 Test Data Week 2

The test data sets contained attacks from five categories that were: Denial of Service (DoS), User to Root (U2R), Remote to Local (R2L), Probe and Data.

At the end of the testing, results of the testing were compiled and the detection rates for the four configurations were calculated. An evaluation was performed and

performance ranking conferred to the different configurations based on the test results. In addition, weaknesses of past evaluations were also highlighted.

1.7 Dissertation Organisation

This dissertation is organized as follows:

Chapter 2: Background

This background chapter is a literature review of Unix-based intrusion detection. Firstly, it deliberates on computer security in general, then, it proceeds to present Unix in the second section. The third section, deals with security in Unix while the fourth section presents the subject of intrusion detection. Finally, it addresses the topic of intrusion detection in Unix.

Chapter 3: Evaluating Intrusion Detection Systems

This chapter discusses three previous evaluations: one from NSS Group, Europe's foremost independent network testing facility and consultancy organisation, and two from the MIT (Massachusetts Institute of Technology) Lincoln Laboratory, under Defense Advanced Research Projects Agency (DARPA) sponsorship. It then introduces the choice IDS tool (Snort), test objectives, test scope and test requirements of this research.

Chapter 4: Test Design

This chapter provides an overview of the testing, describes the attacks in the test data, lists the attacks in each test data set and discusses the steps involved in testing the selected IDS.

Chapter 5: Test Implementation

This chapter provides the information on the test implementation which mainly involves configuring Snort and conducting the test runs.

Chapter 6: Test Results

This chapter presents the results of the testing and the detection rates for the respective Snort configurations.

Chapter 7: Test Evaluation

This chapter is divided into 3 sections; section 7.1 discusses the performance of the four different configurations of the IDS, section 7.2 discusses the performance ranking of the four configurations, and section 7.2 uncovers the flaws of previous IDS evaluations.

Chapter 8: Conclusion and Summary

This chapter summarises the content of the dissertation and presents the conclusion of the research.