8 Summary and Conclusion

Intrusion detection systems are essential in any organisation's computer system security infrastructure. Their performance is evaluated by the rate that their able to detect and report malicious attacks. In this research, four configurations of the selected IDS, called Snort, were evaluated by testing them against tcpdump test data sets that were downloaded from http://www.ll.mit.edu/IST/ideval, within the test environment constructed.

The test environment constructed consisted of:

- The test machine
- Test data sets
- The Unix-based operating system (Linux 8.0)
- Snort (the selected IDS)
- SnortSnarf (IDS Alerts Reporter)
- The Result Forms

The test data sets comprised of a variety of attacks and background traffic. The attacks came from the five following categories:

- Denial of Service (DoS)
- Probe
- User to Root (U2R)
- Remote to Local (R2L)
- Data

Upon completion of testing and gathering of results, each of the four Snort configurations was evaluated whereby their performance ranking was assigned as follows:

- Ranking No. 1 – Snort 1.8.3 Full (43% detection rate)
- Ranking No. 2 – Snort 1.8.3 Custom (41% detection rate)
- Ranking No. 3 – Snort 1.7 Full (21% detection rate)
- Ranking No. 4 – Snort 1.7 Custom (6% detection rate)

In addition to evaluating the performance of the IDS, a study based on the experience of testing end evaluating was performed to reveal the weaknesses of three past evaluations on IDSs. The past evaluations analyzed here were: 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 weakness of the NSS Group evaluation had to do with the background traffic generated and its lack of testing for false alerts. The weakness of the 1998 DARPA-LL evaluations was leaving out Windows NT and not executing malicious attacks in a logical order. The weakness of the 1999 DARPA-LL evaluations had to do with the fact that artificial traffic was used in the test bed and not separating the evaluations between the host-based and network-based IDSs.

In conclusion, the three objectives of the research, mentioned in sections 1.4 and 3.3, were accomplished. The first and second objectives are interrelated. The first objective was to present a method of performing an evaluation of intrusion detection

systems without the use of complex computing resources. The second objective was to evaluate the performance of the four configurations of the selected intrusion detection system, Snort. For this purpose, a testing process that ran four publicly available test data sets through four configurations of Snort on one test machine was performed. The testing process consisted of the following steps:

1. Construction of test environment.
2. Implementation of tests.
3. Gathering of results.
4. Evaluation based on test results.

The evaluation mentioned in step 4 of the testing process is addressed in chapter 7 on Test Evaluation. Finally, the third objective, to uncover the limitations of the three past evaluations, was addressed in section 7.3.