Table of Contents

1. **Introduction** **1**

2. **Intrusion Detection Systems** **2**
   2.1 Types of Intrusion Detection Systems 2
     2.1.1 Host based intrusion detection systems 2
     2.1.2 Network based intrusion detection systems 3
     2.1.3 Hybrid based intrusion detection systems 4
   2.2 Types of Network Attacks 4

3. **Hierarchical Task Analysis** **6**
   3.1 Network Security Administrator 7
   3.2 Functions of Network Security Administrator 7

4. **Diagrams** **9***

5. **Task Descriptions** **17**
   Develop security policy 17
   Select a intrusion detection system 28
   Harden and secure network and servers 31
   Prepare for intrusion detection 44
   Detect intrusion 55
   Respond to intrusion 68
   Improve 76

6. **Validation of Task Analysis** **80**
   6.1 Results of Validation 81

7. **Conclusion and Further Steps** **84**

8. **References** **85**

9. **Bibliography** **86**

* Diagrams are also attached (as TIFF files) to the PDF file.