

A STUDY ON IDS OF A PROTOTYPE HOST-BASED IDS WITH SELECTIVE FILTERING CAPABILITIES THAT FILTER OUT PACKETS FROM ACCESSING THE HOST

Prepared by: Lu Jim Mie

ABSTRACT

The aim of this project is to study on Intrusion Detection System (IDS). This study includes the concepts used by IDS, intrusion detection techniques that are used today to identify if an intruder has illegally accessed the network and how IDS is implemented into networks. A prototype system is also to be developed which would include a host based IDS model to detect anomalous packets entering a host and to filter them out. The developed prototype should also include a logging feature so that users are able to identify attacks being directed to their personal computer. An Internet Protocol (IP) back tracing feature is also included so that users will know where attacks are originating. Additional features might include packet blocking where harmful packets are disallowed from entering the host computer. The developed prototype is targeted at system administrators as well as any normal users who would like to have their network access safe from any harmful intrusions that could damage important data in their computers.