International J. of Engg. Research & Indu. Appls. (IJERIA).
ISSN 0974-1518, Vol.2, No.I (2009), pp 259-269

APPLYING HONEYNET LIKE TECHNIQUES IN ENHANCING THE PERFORMANCE OF HOST-BASED ANOMALY INTRUSION DETECTION SYSTEMS

SOLAHUDDIN B. SHAMSUDDIN AND MICHAEL E. WOODWARD

Abstract

This paper describes a new approach in modelling Intrusion Detection Systems by applying honeynet like techniques to enhance the performance of host-based anomaly IDS detection algorithm. The new technique can be used as an add-on technique for any existing host-based anomaly IDS models. Honeynet technique is quite an interesting technique to detect malicious packets but not many researches have been conducted to use it in a non-honeynet environment. The analysis in this paper shows that the performance of our Protocol-based Packet Header Anomaly Detection (PbPHAD) IDS model can indeed be improved by correlating interesting events that happened at network level to the host to assist the host in identifying an attack. This discovery presents a significant contribution in the form of a novel approach in attack identification using honeynet like technique in a non-honeynet environment. The philosophies and the mechanics on applying honeynet techniques to a host-based anomaly IDS will be the gist of the discussion.

Keywords: Anomaly detection, Honeynet like technique, Intrusion Detection System