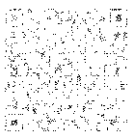
前瞻科技與管理　5卷1期，107-128頁（2015年5月）
Journal of Advanced Technology and Management Vol.5, No.1, 107-128 (May, 2015)
DOI: 10.3966/222014242015050501005

網路入侵偵測的證據萃取與保留的兩階段分析方法

林顥宗[1]　王勝德[2,*]

[1]國立臺灣大學電機工程學系碩士班研究生
[2]國立臺灣大學電機工程學系教授



摘要

入侵偵測系統（Intrusion Detection Systems, IDS）常做為網路分析及監控網路活動以防止入侵的工具。依據入侵偵測的警示，本研究提出2階段分析方法來自動分析網路流量負載，以發掘網路安全問題。第一階段目的在萃取入侵偵測系統（IDS）警示及蓄意的攻擊之間的關係，第二階段則執行特定攻擊的調查與分析。我們的研究目標包含動態蒐集相關證據、嘗試發掘那些以特徵為基礎的入侵偵測系統（Signature-based IDS）所忽略的攻擊手法，以及減少儲存證據所需要的空間。在使用知名資料集的實驗中，本研究提出在不同入侵偵測系統（IDS）組態下的方法及執行效率分析，實驗結果顯示本論文所提方法有能力自動萃取相關證據及節省儲存空間。

關鍵詞：入侵偵測、攻擊防禦圖、警示相關、網路封包、網路鑑識

* 通訊作者：王勝德
電子郵件：sdwang@ntu.edu.tw

前瞻科技與管理　5卷1期，107-128頁（2015年5月）
Journal of Advanced Technology and Management Vol.5, No.1, 107-128 (May, 2015)

A Two-Phase Analysis Approach to Extracting and Preserving Relevant Evidences from NIDS Alerts

Hao-Tsung Lin[1], Sheng-De Wang[2,*]
[1]Master Student, Department of Electrical Engineering, National Taiwan University
[2]Professor, Department of Electrical Engineering, National Taiwan University

Abstract

Intrusion detection systems (IDS) are often used as a network tool to monitor network activities. Based on intrusion detection alerts, we propose a two-phase analysis approach to automatically analyze the network flow payloads. The first phase aims to extract the relations among IDS alerts and discover the suspicious attacks. In the second phase, the investigation of a specific attack is carried out. The objectives of our approach include collecting relevant evidence dynamically, trying to discover the attacks missed by the signature-based IDS, and reducing data storage required to keep the evidences. In the experiments with well-known data sets, the performance of our approach under different IDS configurations has also been analyzed and presented in this paper. The experimental results show that our analysis approach has ability to automatically extract relevant evidence and save more storage space.

Keywords: intrusion detection, attack-defense graph, alert correlation, IP packet, network forensics