Accepted Manuscript

Intelligent intrusion detection systems using artificial neural networks

Alex Shenfield, David Day, Aladdin Ayesh

PII: S2405-9595(18)30049-3
DOI: https://doi.org/10.1016/j.icte.2018.04.003
Reference: ICTE 149

To appear in: *ICT Express*

Received date : 6 February 2018
Accepted date : 9 April 2018

Please cite this article as: A. Shenfield, D. Day, A. Ayesh, Intelligent intrusion detection systems using artificial neural networks, *ICT Express* (2018), https://doi.org/10.1016/j.icte.2018.04.003

Intelligent Intrusion Detection Systems using Artificial Neural Networks

Alex Shenfield
Department of Engineering and Mathematics
Sheffield Hallam University
Sheffield
UK
Email: a.shenfield@shu.ac.uk

David Day
Department of Computing
De Montfort University
Leicester
UK
Email: david.day@dmu.ac.uk

Aladdin Ayesh
Department of Computing
De Montfort University
Leicester
UK
Email: aayesh@dmu.ac.uk

***Abstract*—This paper presents a novel approach to detection of malicious network traffic using artificial neural networks suitable for use in deep packet inspection based intrusion detection systems. Experimental results using a range of typical benign network traffic data (images, dynamic link library files, and a selection of other miscellaneous files such as logs, music files, and word processing documents) and malicious shell code files sourced from the online exploit and vulnerability repository exploitdb [1], have show that the proposed artificial neural network architecture is able to distinguish between benign and malicious network traffic accurately.**

The proposed artificial neural network architecture obtains an average accuracy of 98%, an average area under the receiver operator characteristic curve of 0.98, and an average false positive rate of less than 2% in repeated 10-fold cross-validation. This shows that the proposed classification technique is robust, accurate, and precise. The novel approach to malicious network traffic detection proposed in this paper has the potential to significantly enhance the utility of intrusion detection systems applied to both conventional network traffic analysis and network traffic analysis for cyber-physical systems such as smart-grids.

I. Introduction

Network Intrusion Detection Systems (NIDS) are essential in modern computing infrastructure to help monitor and identify undesirable and malicious network traffic (such as unauthorised system access or poorly configured systems). The majority of commercial NIDS are signature based, where a set of rules are used to determine what constitutes undesirable network traffic by monitoring patterns in that traffic. Whilst such systems are highly effective against known threats, signature based detection fails when attack vectors are unknown or known attacks are modified to get around such rules [18].

As well as struggling to identify unknown or modified threats, signature based detection in NIDS in real-world scenarios are frequently plagued by false positives. This is particularly problematic in the detection of malicious shellcode - a high impact threat vector allowing attackers to obtain unauthorised commandline access to both conventional computer systems and cyber-physical systems such as smart grid infrastructure - as shellcode patterns can be difficult to distinguish from benign network traffic [16].For example, while working as a network security consultant for the Shop Direct Group (UK) using the network intrusion detection tools Sguil and Snort from the Debian based Linux distribution Security Onion, it was noticed that signatures designed to match shellcode frequently also matched other non shellcode binaries e.g. dlls as well as jpg image files. The frequency of these false positives was such that the signatures themselves ultimately had to be disabled, rendering them useless. This experience with the false positive problem with shellcode and signature based systems is very common, Microsoft discuss this at length in their patent of methods to detect malicious shellcode with reduced false positives in memory [16].

Shellcode is frequently used as a payload in system penetration tools due to the enhanced access and further leverage they offer to an attacker [13].

This paper outlines a non-signature based detection mechanism for malicious shellcode based around Artificial Neural Networks. Results presented show that this novel classification approach is capable of detecting shellcode with extremely high accuracy and minimal numbers of false positives. The proposed approach is validated using repeated 10-fold cross-validation and is then tested with respect to creation of false positive alerts on a large dataset of typical network traffic file contents (achieving a false positive rate of less than 2%).

The rest of this paper is organized as follows: section II provides a background to intrusion detection systems and artificial neural networks, before section III provides a brief introduction to the particular instances that motivated the creation of this system and the results achieved by the proposed AI based intrusion detection system. Section IV then concludes with the main achievements of this research and some potential avenues for further work.

II. Background and Previous Work

A. Intrusion Detection Systems

The primary aim of an Intrusion Detection System (IDS) is to identify when a malefactor is attempting to compromise the operation of a system. That is to say, cause the system to operate in a manner which it was not designed to do. This could take the form of a compromise to the confidentiality, availability and integrity of the system and the data stored and controlled by it. Systems could be hosts, servers, Internet of Things (IoT) devices, routers or other intermediary devices