Title: A RASPBERRY PI 3 DEVICE USED AS HARDWARE FOR SNORT INTRUSION DETECTION SOFTWARE

Abstract:

Intrusion Detection Systems (IDS) are becoming more expensive as the technology gets more robust. Many of the costs associated with the systems are incurred by the hardware needed to house the rulesets as well as the data sets that are captured. Because the necessity for an IDS to monitor a company’s network consistently from unwanted attacks. The need for a piece of equipment that will stand the test of time is evident. Alongside the need for a more stable piece of hardware, comes the need for a more technically savvy team of engineers to monitor the system. This is typically built into the total cost of the system that is being purchased. Companies that sell these systems have teams on their payroll that are available to help monitor the systems and/or act as a second level support system for the purchaser. With the costs associated with these services some IDS’s can come in at a cost of over ten thousand dollars.

I am proposing using a raspberry Pi 3 device to house a freeware version of an IDS known as SNORT. The benefits that could come from this type of a setup would be lower cost upfront for the purchasing company. A Raspberry Pi 3 device can be purchased for thirty-five dollars at some online retailers. Add that with SNORT software that is free to download, a company could then “stockpile” multiple IDS devices within their company headquarters. Another possible advantage that could come from this type of a setup is the ability for companies to purchase multiple devices. This will allow them to install multiple devices on the network and use the information gathered from many points of reference within the network to possibly find certain patterns for different types of signatures found incoming to the network. If enough data could be housed its proposed that a pattern could be found with certain types of malware, ransomware etc. and their attack vectors along with the path of attack after the malware enters the network.

This information could give companies a new look at the possible vulnerabilities in the networks. Also, this could help in the mitigation of certain malware signatures before they attack a network. This would hopefully help in slowing down the frequency of attacks on networks in the public.