Network Intrusion Detection System for Virtual Machine base Datacenter Architecture

Shaune Selvathasan

Reg. No: MS20910204

M.Sc. in IT

Specialized in Cyber Security

Supervisor: Dr. Lakmal Rupasighe

December 2021

Department of Computer Science

Faculty of Graduate Studies & Research Sri Lanka

Sri Lanka Institute of Information Technology

Abstract

Now a days most Banks and Finance sectors company are maintain their own inhouse datacenter. For this the main technology there have used is virtualization. Ex: ESXI, Sun Oracle, Citrix and Microsoft Hyper-V. Because of that, these companies must make sure of the server and network security are in a good level. To do that they have to have proper Firewall setup, Core Switch for the server side and the LAN side with Access Control Lists (ACL). Most of the companies have only the Firewall. To prevent a malicious attack or any intrusion attack they are using the firewall. But firewall perform blocking and filtering of traffic through a Network Intrusion Detection System identifies and alert a system administrator or inhibit the attack as per configuration. Firewall allow the traffic based on set of policies that configured by the system administrator. This is where the Network Intrusion Detection System needs in middle of firewall and the server network. Since there is an attack, botnet or malicious thing happened there is no way to stop and prevent or hold the situation automatically. Firewall can only have the alert facility. But if there is a Network Intrusion Detection System it has the prevent or hold capability.

This Network Intrusion Detection System can have deep packets and it use 6 layers of the Open Systems Interconnection (OSI). In this paper I am going to implement a signature base Network Intrusion Detection System with packet filter option, and we can improve overall network security for the server side and for the LAN side also. Here I am going to use Snort, Suricata, open-source firewall using Linux with IPTABLE commands and pfSense Firewall.

Snort and Suricata is an Intrusion Detection System (IDS) that is important to network security. Both of the systems are working together with a firewall.

Keywords – Virtualization, NIDS, Firewall, IPS, Snort, pfSence, Suricata, Security, Microvisor, hypercalls

Contents

List of Figures

List of Tables