



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 Rupasinghe

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, pfSense, Suricata, Security, Microvisor, hypercalls

Contents

Abstract.....	2
List of Figures	6
List of Tables	7
Chapter 1 Introduction	8
1.1 Network Intrusion Detection System.....	9
1.2 Intrusion Detection System Measurement Criteria.....	9
1.3 Intrusion Detection System Mechanism for Information and Data Collection	10
Chapter 2 Virtualization	12
2.1 Virtualization with Full	12
2.2 Virtualization with Paravirtualization	12
2.3 Virtualization with Application	13
2.4 Virtualization Hardware	13
2.5 Virtualization Resources	13
2.5.1 VM Storage.....	14
2.6 Components in Virtualization	14
2.7 Architectures of Virtualization	15
2.7.1 I Method.....	16
2.7.2 II Method.....	16
2.8 Mechanisms of the Virtualization	17
2.8.1 Intel Emulation.....	17
2.8.2 Virtualization Partially.....	18
2.8.3 Virtualization in Operating System-Level.....	19
2.8.4 Paravirtualization and Full	22
Chapter 3 Security of the Virtual Servers.....	27
3.1 Host and Virtual Machine Communication.....	27
3.2 Virtual Machine Escape.....	28
3.3 Monitoring the Host from Virtual Machine	28
3.4 Monitoring Virtual Machine form another Virtual Machine	29
3.5 DoS (Denial of Service).....	30
3.6 Attack Guest to Guest	30
3.7 Virtual Machin Modified by Externally	30
3.8 Hypervisor Modified by Externally.....	31
3.9 Mobility	31
3.10 Intrusion for Hypervisors	31

3.11 Abstraction of Resources	32
3.12 Server Physical Resources	33
3.13 Server System Resources	35
Chapter 4 Security Maintenance of the Virtual Servers	36
4.1 Virtual Machin Sprawl	36
4.2 Configures with Uniqueness	37
4.3 Restore Status	37
4.4 Transience	38
4.5 Testing of the Security	38
4.5.1 Vulnerabilities in Hypervisors Statically	38
4.6 Coddng Analysis of Hypervisor	39
4.7 Peculiarities of Virtualization	40
4.7.1 Detection of Virtualization	40
4.8 Virtualization Protection	42
4.8.1 Isolation of the Control Flow	42
4.8.2 Disaggregation of Hypervisors	43
4.8.3 Management of Memory	43
4.8.4 Technologies use for Networking	44
4.9 Security Architectures	45
4.9.1 Micro Power Hypervisors	45
4.9.2 Virtualization using Nest	47
4.10 Security Mechanisms with Layers	48
4.11 Virtual Machines Protecting	49
Chapter 5 Literature Elaboration and Background	50
5.1 Firewall	50
5.2 NIDS (Network Intrusion Detection System)	51
5.3 IDS (Intrusion Detection System)	52
5.4 Signature Based Detection	54
5.5 Misuse Detection	55
5.6 Anomaly Intrusion Detection	56
5.7 Analysis Stateful Protocol	57
5.8 Intrusion Detection Types	57
5.8.1 Network Base IDS	57
5.8.2 IDS with Wireless	58
5.8.3 Anomaly Detection with Network Behavior	58

5.8.4 Host Base Intrusion Detection System.....	58
5.9 Malware and Botnet blocking system	59
5.10 IPS (Intrusion Prevention System)	59
5.11 Intrusion Detection System vs Intrusion Prevention System	60
Chapter 6 Reference	61

List of Figures

Figure 1 VM Structure.....	14
Figure 2 Restore to State of Malicious.....	37
Figure 3. Firewall Architecture.....	51
Figure 4. Infrastructure of Intrusion Detection System	53

List of Tables

Table 1 Detection Systems in this Network Intrusion Detection System 52