Virtualization in Network Intrusion Detection Systems

Monis Akhlaq[1], Faeiz Alserhani[1], Irfan U. Awan[1], Andrea J. Cullen[1], John Mellor[1], and Pravin Mirchandani[2]

[1] Informatics Research Institute, University of Bradford, Bradford, BD7 1DP, United Kingdom
{m.akhlaq2,f.m.f.alserhani,i.u.awan, j.e.mellor,a.j.cullen}@bradford.ac.uk
[2] Syphan Technologies
pmirchandani@syphan.com
www.syphan.com

Abstract. This research work has focussed on analysing the efficacy of the virtualization concept for Network Intrusion Detection Systems (NIDS) in the high-speed environment. We have selected an open source NIDS, Snort for evaluation. Snort has been evaluated on virtual systems built on Windows XP SP2, Linux 2.6 and Free BSD 7.1 platforms. Our results have identified a strong performance limitation of NIDS running on virtual platforms. This can be concluded that virtualization is not an ideal solution for NIDS in high-speed environments.

1 Introduction

Our research work focuses on evaluating the virtualization concept for NIDS in high-speed networks. Virtualization has found its acceptance in NIDS; however no comprehensive evaluation has done before. Mostly, the concept has been debated on perceived logics of resource conservation in virtualization without any experimental proof. We have analyzed the concept by utilizing open source NIDS- Snort under high-speed multi-Gbps environment. Snort [1], an open source NIDS has been selected because of its popularity and status as a *de facto* IDS standard. Snort relies on the packet capturing libraries (libpcap and winpcap) [2]. Our concept is unique in the sense that we have incorporated three different OS platforms and the evaluation criteria are based on packet handling capacity of Snort. Our effort in [3] describes the comprehensive evaluation methodology with in-depth analysis of the factors responsible for virtualization limitation in NIDS in high speed environment.

2 Methodology

The evaluation technique is based on analyzing the ability of virtual system in terms of their packet capturing capability. The test-bench is distributed into three parts: traffic generation, traffic reception and the Snort virtual platform configured on a dual quad-core processor. The system is built on the Windows 2008 Server platform and three separate virtual platforms have been created-Windows XP SP2, Linux 2.6 &

R. Meersman, P. Herrero, and T. Dillon (Eds.): OTM 2009 Workshops, LNCS 5872, pp. 6–8, 2009.

Free BSD 7.1. Snort is running simultaneously on all the virtual machines and similar traffic-loads and types are injected onto all platforms.

3 Results

3.1 UDP Traffic – Packet Sizes 512 and 1024 Byte at 100 Mbps to 2.0 Gbps

- Linux shows quite good performance for traffic-load upto 500 Mbps for all packet sizes. The Linux however system found non responsive at traffic-loads of 1.0 Gbps and above for 512 Bytes packet sizes and at 2.0 Gbps for packet sizes of 1024 Bytes.
- Windows also performed satisfactorily at traffic-loads of 250 Mbps and 500 Mbps for packet sizes of 512 Bytes and 1024 Bytes respectively. The system found non responsive at traffic-loads of 1.0 Gbps and above for packet size of 512 Bytes and 2.0 Gbps for packet sizes of 1024 Bytes.
- Free BSD responds a bit better than Windows, the system found non responsive at traffic-loads greater than 1.0 Gbps for packet sizes of 512 Bytes and 2.0 Gbps for packet sizes of 1024 Bytes.

3.2 TCP Traffic – Packet Size 512 Byte for 100/ 200 Connections

- Linux exhibits quite good performance upto 250 Mbps loading with minimum packet loss, however, its response linearly declined for higher traffic-loads.
- Windows also exhibits a similar performance level upto 250 Mbps loading levels and its performance declined for higher traffic-loads.
- Free BSD performs a bit better than Windows.

4 Conclusion

The results obtained have shown a number of significant limitations in the use of virtual NIDS, where both packet-handling and processing capabilities at different traffic loads were used as the primary criteria for defining system performance. We have confirmed that the underlying host hardware plays a prominent role in determining overall system performance. We have further shown that performance is further degraded as the number of virtual instances of NIDS is increased, irrespective of the virtual OS used. Furthermore, we have demonstrated a number of significant differences in the performance characteristics of the three different virtual OS environments in which Snort was run.

This work has identified specific and replicable bottlenecks in commonly used implementations of virtualization for a widely used NIDS in high-speed networks. The results obtained can be taken as a benchmark for improving the performance of these systems in future research work. These shall also provide an experimental data to the researchers which were felt missing in the previous efforts.

References

1. Snort, http://www.Snort.org/
2. Baker, A.R., Esler, J.: Snort IDS and IPS Toolkit. Syngress, Canada (2007)
3. Akhlaq, M., et al.: Virtualization Efficacy for NIDS in High Speed Environments. In: Information Security and Digital Forensics Conference 2009 to be held in City University London, September 7-8 (in press, 2009)