Virtualization Technology Whitepaper - Infrastructure to Perform Static Tools and Binary Analysis

By: Tommy Gain

February 12, 2017

325 Gambrills Road, Suite D,
Gambrills, Maryland 21054
410-439-1944 P/410-439-1945 F
www.fuseENG.com

Table of Contents

325 Gambrills Road, Suite D, Gambrills, Maryland 21054
410-439-1944 P/410-439-1945 F
www.fuseENG.com

Executive Summary

Software assurance professionals require a platform to test open source programs and live malware analysis; a segregated lab aimed at improving the capabilities of testing tools, identify and spot weaknesses in software. Virtualization technology provides the ability to build and maintain a completely sandboxed and air gapped network. A virtualized infrastructure provides a high-performance platform, completely customizable for its users. By providing a comprehensive infrastructure solution for software analysis, we reduce the risk for incorporating effective quality assurance into the software development lifecycle.

Introduction

Finding software flaws and analyzing live malware data sets is a challenge in any secured or corporate environment. Organizations have strict security guidelines to follow and software engineers and software assurance professionals are rarely given the tools they need and the open freedom required to perform this task. Building test networks, servers, clients, and install the required tools is not only expensive, but also a challenge in a secure environment because of the strict security requirements and the introduction process of these tools. We know tools have different strengths, and no one tool can find all types of weaknesses. A National Institute of Standards and Technology study found that it is rare for the same defect to be detected by three or more tools (Kuhn, Kacker, Lei,. 2010). We recently provided support for a software assurance organization tasked with finding software defects. Their efforts resulted in a study of

60,000 test cases with nearly 10 million lines of C, C++, and Java code. Through this analysis, they found that only 14% of known software defects were detected, even with multiple tools.

How were they able to perform so many test cases using these tools without compromising the enterprise network? How did they comply with enterprise security guidelines? These tests were conducted on a sandboxed, air gapped network, utilizing VMware ESXI Hypervisors and VMware virtualization technology. This type of sandboxed environment allows for little to no downtime in recovery in case of malicious virus takeover. "Virtualization is the process of creating a software-based (or virtual) representation of something rather than a physical one. Virtualization applies to applications, servers, storage, and networks, and is the single most effective way to reduce IT expenses while boosting efficiency and agility for all size businesses" (What is Virtualization. 2007). This virtual infrastructure is used to improve performances through a standardized platform normalizing the results from multiple static analysis tools. Software assurance professionals do not have to calibrate and configure the tools, and the results are standardized using CodeDX, which consolidates and normalizes vulnerabilities detected by different tools.

Problem Statement

Software assurance professionals need an environment in which they can create private or public networks to test software; quickly spin up networks, servers, clients; and install the required tools quickly and efficiently without restrictive "red tape". Malicious software is morphing to be more targeted, stealthy, and destructive, which means this software cannot be tested and researched on common networks which leave enterprise programs at risk.

Solution

We utilize commercial vendor products such as Cisco for routing and switching, hardware platforms like Dell for hypervisors, and VMware software to create a standardized infrastructure capable of providing access and ability to software evaluation professionals.

We build bare metal infrastructure solutions including the implementation of routers, switches, networked together hypervisors, and VMware Technology. The software assurance professionals then connect to this network resource, providing the ability to perform quick run-time analysis of live malware, documenting the network behavior of unknown malware samples. We specifically configure server service implementations like Apache, Postfix, dnsmasq and ntpd. We use VMware ESXI Hypervisors and VMware Virtualization Technology (V/T), allowing software assurance professionals to engineer custom networks, vlans, distributed switches, and choose which operating system they'll need to perform the analysis. This completely custom virtualize network can be built in hours, and it can be deleted and rebuilt to ensure a clean environment for the next test.

Conclusion

Utilizing V/T, IT system administrators are able to assist software assurance professionals to engineer custom scale, diverse, and complex infrastructures atypical to modern enterprise. This allows for hybrid and multi-OS environments, application installation, and code review, without security threats running rampant on enterprise networks and systems. Virtualization increases IT agility, flexibility, and scalability while creating a significant cost savings. Workloads get

deployed faster, performance and availability increases and operations become automated, resulting in IT that's simpler to manage and less costly to own and operate.

Resources

D. R. Kuhn, R. N. Kacker, and Y. Lei. (2010). Practical Combinatorial Testing, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-142, 82 pp.

What is Virtualization. (2007). http://www.vmware.com/solutions/virtualization.html