Evaluation of Network Security on basis of Virtualization Techniques in Kali Linux Environment

Prof. Vinit A. Sinha[a], Dr. V.M. Thakare [b]

[a] Assistant Professor, vinit.sinha84@gmail.com
[b] Professor and Head, vilthakare@yahoo.co.in

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 4 June 2021

Abstract: In today's cyber security space network security has a top priority specially system based on Open Source platform. Kali Linux is the new door for white hat security specialist for hardening security for firm and organization. Kali is secure based distribution from linux family having Debian platform. As it includes over 600 + preinstall security application, so it is needy to keep record of network activity by the system and to the system. As kali linux is power tool for server security, virtualization is secure way to implement that tool. The main purpose of this article to evaluate network security on basis of virtualization techniques for this we track implementation of KVM (Kernel Based Virtual Machine) using three virtualization techniques – virt-manager, kimchi project and SDN (Software Defined Network).

Virt-manager is python-based desktop user interface for editing and customization of virtual machine through lib-virt. Kimchi is HTML based virtual machine management tool specially used for KVM. SDN is a technology revaluation which needed priory in cloud and virtualization world for providing network services. In this paper we aim to present advantages of virtualization techniques to explore network security hardening in kali linux.

Keywords: Kali linux, Kimchi, KVM, SDN, Virt-manager.

1. Introduction

Virtualization in network security is a new era. KVM and linux environment specially kali linux are key elements of network security. Problems arises while selecting a proper flavor of linux for server building are administration security [1], tools configuration, hosting capacity, client request response and hardware support for service providence. For its great security tool support Kali linux is well known, So, it is network demand to host web server on Kali in virtual manner.

In this paper we evaluate performance of virtualization techniques to build strong network policies, with hosting to numerous applications including hardware support.

As shown in Fig. 1, virtual architecture is differing than traditional architecture, which has additional layer and extended to subcategories of operating system and application for effective use of system hardware and extent use of Host Operating System (OS).

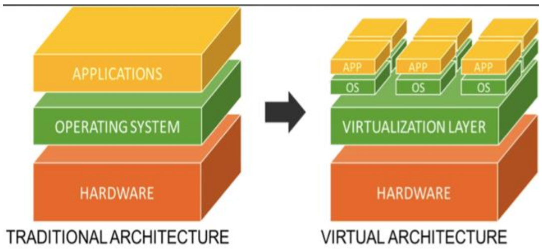

Fig. 1: Virtualization Architecture

This paper is organized as, Section 2 discusses about related work, which provides details of virtualization in network security, Section 3 discusses on methodologies which includes details of virtualization techniques as 3.1 – Virt-manager ; 3.2 – Kimchi Project ; 3.3 – SDN , Section 4 discusses about implementation of virtual machines, Section 5 report about result and evaluation and last Section 6 conclude the paper.

2. Related Work

This section discusses about the literature survey of different researchers in the field of virtualization and network security. The researcher Ganji et al. [2] examined suitable infrastructure for the linux OS. They also mentioned linux system security requirements in server network security. Patil et al. [3] proposed hypervisor level distributed network security (HLDNS) framework which is deploy to monitor VM related network traffic for intrusion detection. Li et al. [4] proposed framework, which divides network security into five stages which are as factor acquisition, model representation, measurement establishment, solution analysis and situation prediction. Bock et al. [5] explain real time hypervisor based on Xvisor for delivering secure and separated environment for virtualized system. Compastie et al. [6] describe comparison between different virtualization models to build architecture of cloud infrastructure for analyzing network security issues. Yan et al. [7] verified effectiveness of system using client-side distributed energy storage demo project for improving system load characteristics. Potdar et al. [8] describes server virtualization, which provides a platform to run different OS services. They describe performance evaluation of docker container and virtual machines using effective tools. Bahn et al. [9] explains separations of VM for managing unnecessary network traffic.

3. Methodology

For selecting a kali linux for network security in virtualization is due to its special architecture as shown in Fig. 2 [10].

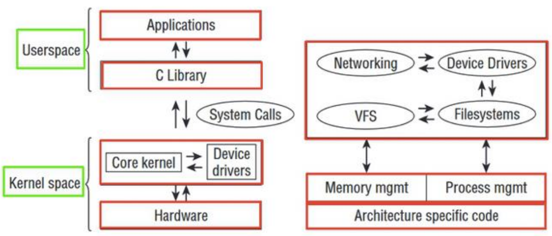

Fig. 2: Kali Linux Architecture

It clears the structure of High-level use in linux system specially kernel. Kali supports specially to VFS (virtual file system) to target virtualization facility. We then evaluate network security in kali linux on basis of following three techniques shown in Fig. 3

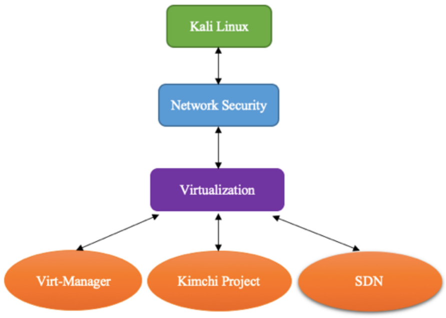

Fig. 3: Three Virtualization Techniques

3.1 Virt-manager:

It is python-based UI for managing virtual machine specially KVM, XEN and LXC containers. It allows users to create, edit, start / stop VM.

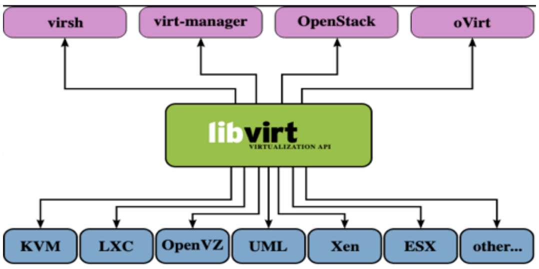

Fig. 4: Virt-Manager

As shown in Fig. 4, virt-manager has different API hands, which use to manage networking Console of different VM.

3.2 Kimchi Project:

Kimchi communicates with libvirt for better virtualization. It is categories in four main modules to facilitate communication between libvirt and Ngnix, which is a web application server to serve user interface. Fig. 5 shows High level architecture use in Kimchi.

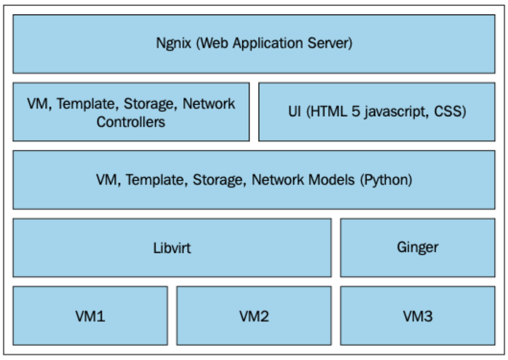

Fig. 5: Kimchi Architecture

3.3 SDN (Software Define Network):

SDN is a high value architecture, which is cost effective, dynamic manageable and adoptable by different VM. ONF (Open Flow) protocol is fundamental element of SDN architecture. Fig. 6, differ SDN from traditional network service.

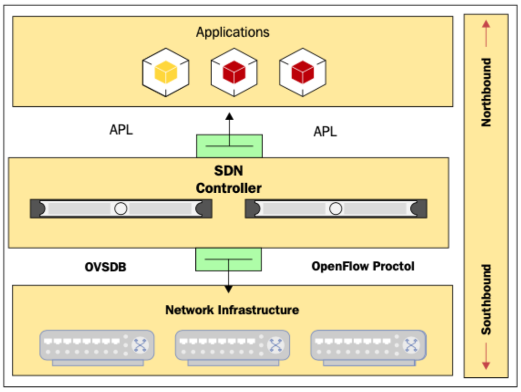

Fig. 6: SDN Architecture

Above figure shows separated control and data planes which helps application to control directly network and give startup to new innovations.

- Network infrastructure - Includes network devices such as switches, routers and bridge couple devices.
- Controller – It is centralized control system setup on server which communicate through all devices in network by OPEN API.
- Applications – This includes variety applications like voice, video, technology-based application and security tools like intrusion detection.

4. Implementation

As mentioned above virtualization techniques solves the problem of limited number of system calls, while security management in (HIDS) describe by Zhang et al. [11].Our describe concept result out wrapping of different security mechanism around Guest OS. As mentioned in Section 2, researchers are tried to provide separate security layer around KVM, which can be apply by using different proxy tools like Cloud VPN [12], Hoxx proxy [13] protocol tools etc.

5. Result And Evaluation

By applying three techniques on KVM for network-based virtualization we get different security results on basis of hardware support, software support and their version upgrade factors and all results are express in terms of scale factors (1-10). The chart view is as shown follows Fig. 7.

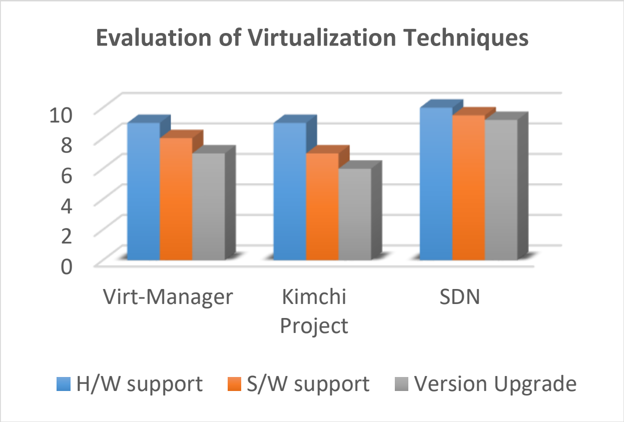

Fig. 7: Chart view of Evaluation

Above mentioned evaluation shows SDN techniques is more effective than virt-manager and Kimchi project with this SDN have additional network infrastructure management and controller.

6. Conclusion And Future Scope

In this paper, we focused on different virtualization techniques and their effective use in network security, which include management of VMs, binding of particular tools required by Kali linux.

In future, virtualization technology can be securely implemented by providing extra kernel support, where SDN based controller can be attack at single point. For this we plan to deploy various security scripts compile in python.

References

[1] Crawley, D. R. (2014). The accidental administrator: Linux server step-by-step configuration guide: edition 2.0b. Soundtraining.net, learning resources for IT pros.

[2] Ganji, H. R., & Aghakhani, K. (2018). Provides a New Way to Enhance Security in the Linux Operating System. Emerging Science Journal, 2(5), 295.

[3] Patil, R., Dudeja, H., & Modi, C. (2019). Designing an efficient security framework for detecting intrusions in virtual network of cloud computing. Computers & Security, 85, 402–422.

[4] Li, Y., Huang, G., Wang, C., & Li, Y. (2019). Analysis framework of network security situational awareness and comparison of implementation methods. EURASIP Journal on Wireless Communications and Networking, 2019(1), 205.

[5] De Bock, Y., Mercelis, S., Broeckhove, J., & Hellinckx, P. (2020). Real-time virtualization with Xvisor. Internet of Things, 11, 100238.

[6] Compastié, M., Badonnel, R., Festor, O., & He, R. (2020). From virtualization security issues to cloud protection opportunities: An in-depth analysis of system virtualization models. Computers & Security, 97, 101905.

[7] Yan, T., Liu, J., Niu, Q., Chen, J., Xu, S., & Niu, M. (2020). Network security protection technology for a cloud energy storage network controller. Global Energy Interconnection, 3(1), 85–97.

[8] Potdar, A. M., D G, N., Kengond, S., & Mulla, M. M. (2020). Performance Evaluation of Docker Container and Virtual Machine. Procedia Computer Science, 171, 1419–1428.

[9] Bahn, H., & Kim, J. (2020). Separation of Virtual Machine I/O in Cloud Systems. IEEE Access, 8, 223756–223764.

[10] System Architecture of Kali Linuxs. (2021). Retrieved 30 March 2021, from https://selflearning.io/study-material/website-penetration-testing/website-penetration-testing/chapter-7-linux-hacking/system-architecture-of-kali-linux.

[11] Zhang, X., Niyaz, Q., Jahan, F., & Sun, W. (2020). Early Detection of Host based Intrusions in Linux Environment. 2020 IEEE International Conference on Electro Information Technology (EIT), 475–479.

[12] What Is a Cloud VPN?. (2021). Retrieved 1 April 2021, from https://www.paloaltonetworks.com/cyberpedia/what-is-a-cloud-vpn

[13] Hoxx VPN Proxy - Free VPN Service. (2021). Retrieved 1 April 2021, from https://hoxx.com/