The 49th Annual IEEE International Carnahan Conference on Security Technology

# Benefit of Construct Information Security Environment Based on Lightweight Virtualization Technology

Jen-Chieh Wang, Wei-Fun Cheng, Han-Chiang Chen, Hung-Li Chien
Department of Information Management Center, National Chung-Shan Institute of Science and Technology
Taoyuan, Taiwan
Email: {pisciscsist, kuas1095108129} @gmail.com , {ericmiau, hungli_chien} @yahoo.com.tw

***Abstract*—Recently, in order to strengthen the capabilities of security defense and emergency coordination, training in a virtual environment is more and more important. In a virtual environment, the trainee can operate the really system. The answer of how to attack or defend is no more just one solution. You can use any method or trick to reach the goal. The outcome of training in a virtual environment can directly prove the trainee's capability. Although there is a lot of advantage to use virtual environment, it's a big problem to build it. The work of creating virtual environment includes allocation and maintenance. To allocation, because training in an environment providing daily service will decrease the performance of service. It's hard to allocate virtual environment in a real environment providing daily service. In order to simulate the real environment, it needs a lot of space and powerful computing. To maintenance, the built virtual environment needs expandable, flexibility and reusable. For example, it can change IP or count/password easily so the test would not always the same and virtual environments can be reusable. For now, it use cloud computing[8] to virtualize the virtual environment to solve the two problem. But there is still a problem of too heavy. In this research, we try to build virtual environment based on Docker which provide manager a structured process to build a virtual environment by building a independent containers and Open vSwitch in the operating system layer. We can monitor the status of virtual environment with charts so the manager can control the system more effective and help researchers or military to do security education.**

***Keywords*—LXC、Docker、Education**

## I. INTRODUCTION

Practicum is an integral part of network security education. In the past, network security teaching experiment environment is usually situational customized, but without flexible and scalable. Therefore, the experiment cannot be implemented in a traditional lab environment when conducting a experiment of new network attacks and defenses. To resolve this type of problem is usually to build a virtual laboratory platform with virtualization technology (such as KVM, XEN and Hyper-V, etc.) in the past. In this paper, we build a virtual environment teaching platform based on Docker which can be rapidly deployed with a large number of containers. Also, utilizing the Open vSwitch to construct the network environmental configurations for the experiment, it will help students to easily perform network teaching or offensive drills and it will also solve the problem of low efficiency of laboratory resources and realities.

## II. RELATED WORK

### A. Virtualization

Virtualization is the host of a variety of server computing resources such as computing power, memory, network and storage space, etc. with virtual configurations of virtual machines or application containers, allows multiple operating systems and applications operating simultaneously on a single physical server (see Figure 1).

Virtualization technology can be broadly divided into three categories that are Full-Virtualization, Para-Virtualization, and OS-Level Virtualization. Full-Virtualization and Para-Virtualization create a virtual machine with Hypervisor. The main difference between these two virtualization is that Full-Virtualization provides as the guest OS is fully abstracted from underlying hardware by virtualization layer, but the Para-Virtualization has direct access a part of hardware resources with privileged instructions[1].

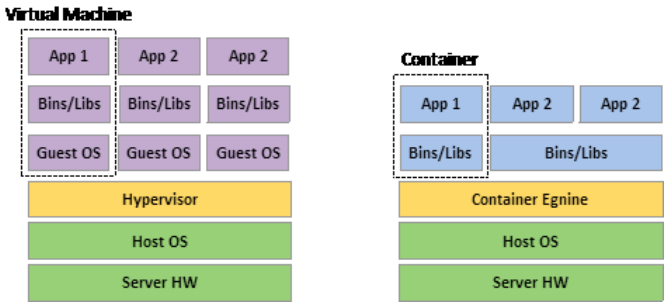


Fig. 1. Virtual Machine V.S Container

OS-Level Virtualization (operating system level virtualization) build a virtual execution environment in operating system core system layer based on sharing Host OS to allocate resources for the Container equipped with applications. The virtualization can reduce the resources consumed by virtualized hardware, that is the Container shares OS core and libraries directly with Hosts (see Table I). Since

each Container is independently isolated with others, each Container own its computing resources, but isolated from each other. Compared to traditional virtualization, Container takes more advantages which is that Container startup within a few seconds with faster speed and smaller space with loading more services[2].

TABLE I. VIRTUALIZATION V.S CONTAINERS

| | Virtualization (i.e. KVM, Xen) | Containers (i.e. LXC, Docker) |
|---|---|---|
| Typical server deployment | 10 – 100 VMs | 100 - 1000 containers |
| Boot time | Less than a minute | Seconds |
| Physical resources | Each VM has resource reserved for its own use | Shared by all containers |

### B. Docker

Docker is Linux Container management integration tools which is utilizing Kernel Namespace and Control groups combined with aufs file system for the Container to achieve operational efficiency approaching a real computer, provide mechanisms with systems layering and version controlling, and take into account the flexibility of system security and data utilization. Docker originally is a internal project in dotCloud company which is to study using lightweight containers but Hypervisors in order to solve the major challenge of resources allocation for environmental services and make services performed independently[3][6][7].

### C. Open vSwitch

Open vSwitch is a source code project to solve the network virtualization developed by Nicira. The goal is easy to manage and deploy of virtual machines and virtual network switches in order to make virtual switches can be managed from external. Also, it is based on supporting extended programming to achieve large-scale network automation and network virtualization and detect traffic information passed through a host in a dynamic virtual environment. The connection between the virtual machines and networks is implemented by a virtual NIC (vNIC) on the virtual machine connected to the virtual switch (vSwitch) or network interface card (NIC) to connect to the internet. These efforts were originally implemented by the linux bridge, but the Open vSwitch provides external support such as Open Flow management mechanism and remote management interface to make it more adopted to the cloud environment[4][5].

## III. SYSTEM ENVIRONMENT PLAN AND DESIGN

In the past, when executing or simulating network attack and defense, independent systems belonged to attacker or defender are customized in order to practice the behavior of network attack and defense. For example, to simulate a web site suffered cyber attacks, you might build web services on a single server or virtual machine and the site may need similar services such as Apache, MySQL, etc. to operate services. In this architecture, the problem is how to expand or better performance in the future and it may easy be clashed due to an error (BUG).Therefore, we will separate each component in the system to make it operating independently and form all components together to run a system later. Take the web site as an example, the web site components, Apache, MySQL serve independently and are formed as a web service based on load balancing (HAproxy) and network configurations. When using the micro-services to construct systems, container is very suitable as the underlying configuration. Because it is more compact and operates more quickly than the virtual machine. Also, it makes the system more scalable (see Figure 2).

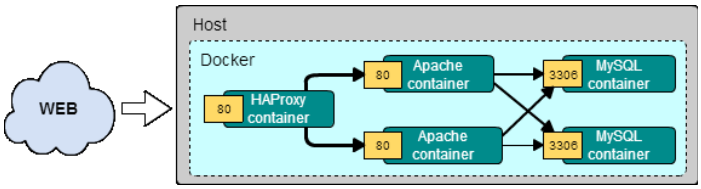


Fig. 2. Containesr & Micro Services

After completing the planning system elements, the image files shall be made. We can make use of Docker to download the base image files from Docker Hub, and apply Docker file to operate Container environment variables, software installation, and permissions setting to produce various micro-services customized firmware image files, and then save them to a private warehouse management. By using of Docker, it not only reduces system deployment time, but also reaches a

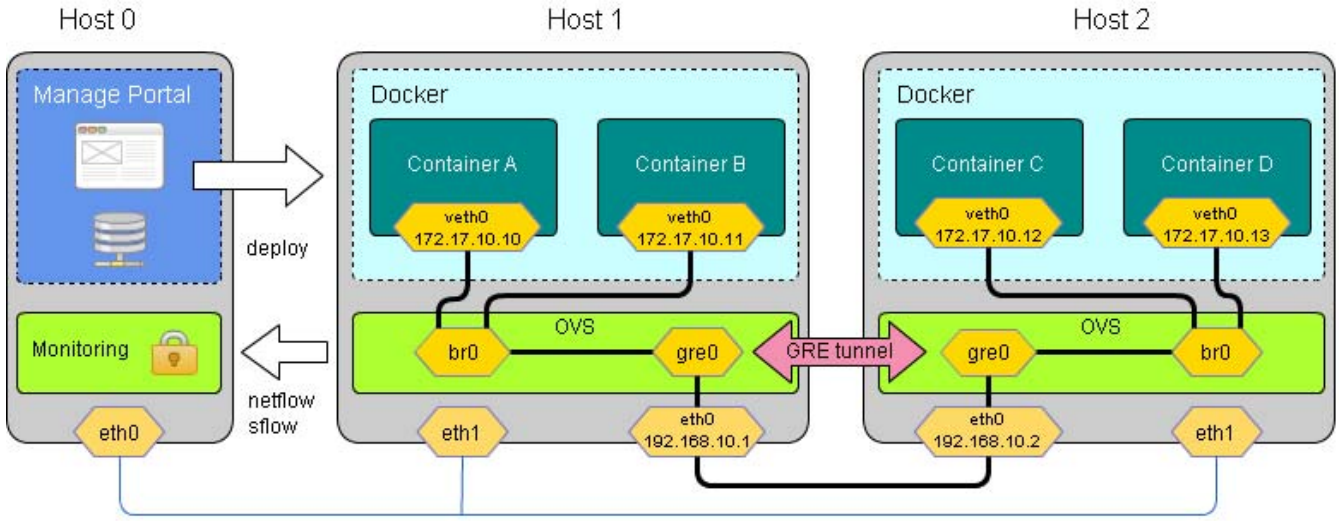


Fig. 3. Experimental infrastructure environment

system automation deployment. Hence, we can focus on the system planning, design and practice offensive and defensive drills.

Based on experimental infrastructure environment (see Figure 3),there are Management Host0, Container Host1 and Host2 Management Host0 establishes Manage Portal to control Dockers in Host1 or Host2 and configure ovs. And, through ovs operation to collect the netflow information of Host1 and Host2 to analyze network traffic. Network configurations between Containers are applied of GRE Tunneling technology to implement based on the Open vSwitch in order to achieve interoperability purposes between Container AB and Container CD. Furthermore, in response to a variety of different environments , VLAN is also applied to manage routing.

## IV. EXPERIMENT

To perform a network offensive and defensive drills or network security education, we must know the difference of effectiveness between simulation and the real world. Thus, we test our cyber attacks DDoS program executed on the same specifications native, virtual machine, and Docker container on the same defense host computer respectively. Because of the defense host computer is windows system, Microsoft has not yet to support container. Therefore, we only compare the effectiveness of cyber attacks program execution and network latency forwarding experiment.

We compare different scenarios as illustrated below, as shown in Figure 4:

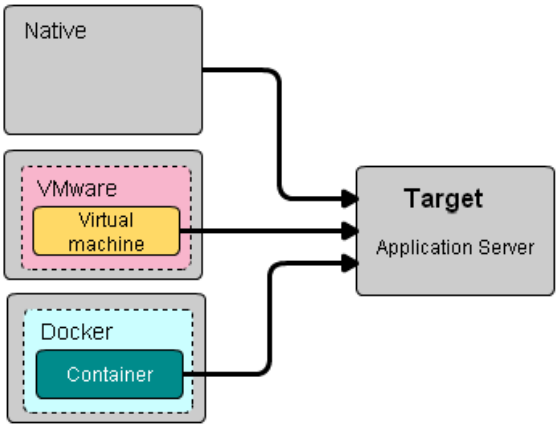


Fig. 4. Experimental schematic diagram

- Native: Linux OS running directly on hardware.
- VM: VMware vSphere 5.5 with the same OS as native.
- Docker: Docker version 1.2 running on a native OS.

For this study, we used the micro-benchmarks listed below:

### A. Application Performance—network attack app

Cyber attacks program will generate a large number of subroutines sending requests to attack targets. The number of requests that cyber attacks program can send are affected due to the level of host performance. We compare the performance of the VM and Docker container based on requests of native (see Figure 5). We can see the effectiveness of Docker container is very close to the native effectiveness. It also works in consistent with the Docker container reducing the simulation of hardware device so that the effectiveness is close to the native.

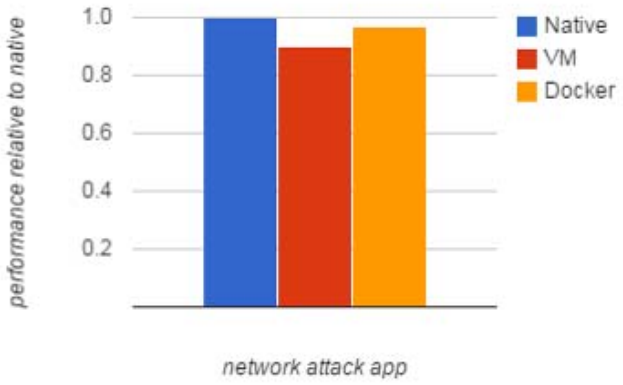


Fig. 5. Network attack application performance relative to native (High is beter)

### B. Network Latency—netperf

Native network of Docker container sent packets to the external are to be forwarded using the docker nat. In this case, we use the Open vSwitch to assist management, implement network behavior analysis, and enhanced the performance of Docker's network transfer. We also use netperf measuring its network latency of packet transmission(see Figure 6). The effectiveness of Docker with the Open vSwitch is not inferior to the virtual machine.

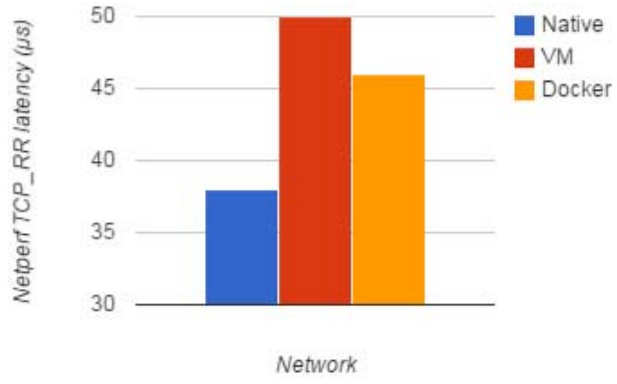


Fig. 6. Network Latency with Netperf TCR_RR (Low is beter)

## V. CONCLUSION

Applying Docker is based on the concept of using micro-services Container in order to build and quickly deploy a large scale of standard test lab environment or system. The demand for resources for a Container is very low, and it can achieve higher performance. In order to simulate a variety of complex network attack and defense scenarios , we apply Docker network combined with Open vSwitch to collect information

of netflow and sFlow based to verify methods of network attack. Under this Docker environment infrastructure, to deploy experimental environment or system is to provide with a high-performance, high scalability, and verification mechanism. However, the Docker container is still inadequate of security controls, but useful tools can be applied to strengthen the base of the Container. Currently, the Docker is getting more widespread attention and discussion, there are more related projects managed on the Docker. We believe that the Docker will be applied more widely with more mature Docker technology.

## REFERENCES


[1] Virtualization, http://en.wikipedia.org/wiki/Virtualization

[2] LXC, https://linuxcontainers.org/

[3] Docker, https://www.docker.com/

[4] Open vSwitch, http://openvswitch.org/

[5] Multi-Host Docker Network , http://wiredcraft.com/blog/multi-host-docker-network/

[6] Example microservice authentication and authorisation solution using Docker containers , https://github.com/stevenalexander/docker-authentication-authorisation

[7] Docker networking basics & coupling with Software Defined Networks , http://www.slideshare.net/adrienblind/docker-networking-basics-using-software-defined-networks

[8] Cloud-Based Virtual Computing Laboratories, Burd, Stephen D. ; Luo, Xin ; Seazzu, Alessandro F. , [10.1109/HICSS.2013.131]