Chapter 2
Handling the Hypervisor Hijacking Attacks on Virtual Cloud Environment

Su Su Win and Mie Mie Su Thwin

2.1 Introduction

Early on year 2000, virus writing was so popular in all ICT ranges. The enormous amounts of virus took place in the field of cyber domain, and millions of hosts are infected. The name of the virus, so-called the Sober virus, infected and spread out over 218 million machines in 7 days. The email virus, Mydoom, was sent to about 100 million of machine as an infected email. The I LOVE YOU virus affected 55 million of machines by gathering usernames and passwords. These attacks were just about boasting, not to earn money.

In the last decade, virus writing is old-fashioned or out-of-date. Then, it was the time of malware and phishing attacks. They were hacker's intentional target for financial purpose by deceiving every individual to get username and password from innocent users.

After that, new-generation, cloud environment will easy to use for the people. Conventional management and control platforms are countering huge challenges concerning with security. So, next-generation systems will require to be more dependent and flexible for more secure cloud environment. The cloud computing architecture model can solve the problem associated with resource utilization, allocation, managements, etc.

However, many elements for example, well-styled architecture of cloud system are still not flexible and difficult to modify, adapt, and change to be associated with this fashion. It consists of crucial network topologies, many components, and

S. S. Win (✉)
Information and Communication Technology Research Centre (ICTRC), Yangon, Myanmar

M. M. S. Thwin
Cyber Security Research Lab, University of Computer Studies, Yangon, Myanmar

G.R. Sinha (ed.), *Advances in Biometrics*,
https://doi.org/10.1007/978-3-030-30436-2_2

dimensions of the user control over infrastructure as a service, platform as a service, or software as a service.

Nowadays, otherwise, in current modern era, we have to move our private information and data from local workstations and servers to cloud computing architecture where all of these data are very attractive and live behind the cloud service provider. So the game of the hacking process is changing and encounters new technical challenges.

Behind the scenes of the cloud computing is virtualization infrastructure. The meaning of virtualization is a construction of virtual (rather than actual) machines which can run multiple operation systems on a single PC or device, but it has to share all hardware resources, for instance, servers, storage devices, network devices, operating system, desktop, and applications virtualization.

The main idea of virtualization is to share IT properties and resources in order to get benefits from abstraction of layers in business, organizations, and all government sectors. The physical machine which creates the virtual machine is referred to as host machine and is also known as a guest machine.

One standard example in virtualization environment is hypervisor. A hypervisor is located in a place between the virtual machines (VMs) and the real physical hardware device. By using this kind of software, layer abstraction separation provides a great chance for system admin to be more flexible when managing and controlling virtual machines.

However, because of the common connection between VMs and physical layer, hypervisor can be regarded as a risk carrier when compromising and propagating of threat and risk. Unlike physical network architectures, it is difficult to see log, countermeasure function like penetration testing (network pen test) and scanning.

The complexity of virtualization with a new challenge is hyper-jacking; the newborn hyper-jacking revolves around the business world's emerging enthusiasm for application, operating system, and issue of virtualization. Hyper-jacking expresses the hypervisor stack jacking. Hyper-jacking involves setting up a rogue hypervisor that can acquire complete control of a server.

Hyper-jacking or hypervisor attack is a great approach not only compromising a server and stealing data but also in maintaining the persistence. As soon as it is getting control of the hypervisor, it can control everything running on the machine. The hypervisor is the single point of failure (SPOF) in cyber security, and if it is lost, protection of sensitive information may also be lost. This increases the degree of risk and exposure may be large. Today, the conventional security monitoring and measure tools are inadequate to harden the operating system, so machine can be compromised. Figure 2.1 shows before installation hypervisor on PC and after attack on a hypervisor.

Although cloud computing has plenty of benefits with virtualization, it brings numerous amount of security vulnerabilities. This paper presents three objectives: firstly, to understand the terms of virtualization vulnerabilities in cloud computing; secondly, to recognize the virtualization threats; and, thirdly, to give the mitigation technique and awareness knowledge for hypervisor attacks and hyper-jacking-style threats that include a particular type of malware called virtual machine-based

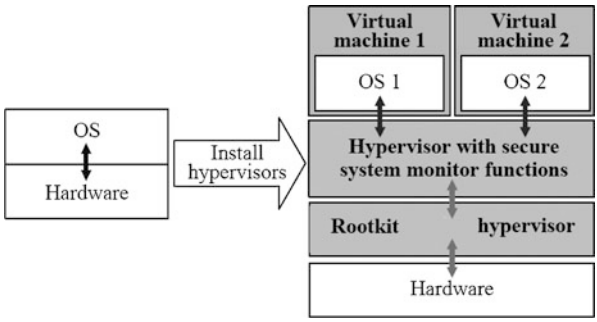

Fig. 2.1 Illustration of layer-wise hypervisor attack

rootkits and also revel avoiding methods with behavior-based hypervisor detecting method.

2.2 Related Works

Till now, central processing unit (CPU) of Intel and AMD processor is vulnerable, and it is difficult to find out with build-in discovery tool to make countermeasure secure hypervisor handling [1]. So this is an important research topic of security issue, and all researchers have to try to solve this kind of challenges. The proposed system reveled exploration, classification, and analysis of vulnerabilities and types of attacks in virtualization environment by using open-source detection software.

The first and foremost of rootkit that happen on hypervisor is started in 2006 and developed by Joanna Rutkowska. The name of the rootkit is so-called Blue Pill [1]; it is the first, real, and effective hypervisor rootkit that used driver based on windows utilized in AMD central processing unit [2]. Similarly, at the same time, in 2006, Dia Zovi was developed MAC OS and Intel central processing unit, and Vitriol. Then, detection on hypervisor started in 2007 [1].

Fannon was presented and made analysis in 2014 to prove that the comparison between two hypervisors [3]. Vitriol and Blue Pill became prominent tools in information technology (IT) security environment and had persuaded the formation of many different hypervisor detection methods and approaches.

The exposure of detection technique can be categorized into four groups: behavior-based, detection-based, signature-based on the trusted hypervisor, and time-based detecting analysis. The technique with signature-based detection utilized memory scanning of hypervisors' design and pattern. The other three categories are based on the interaction and collaboration with a hypervisor [3].

Blue Pill [4] and Vitriol [5] were famous development projects in recent years, when system is in a run time stage that installs and puts in malicious code to the hypervisor. At the primary stage, hypervisor exists as an international standard machine; the above mentioned two projects are able to insert a malicious code to hypervisor on a memory where there is no need to reboot process.

The system of hacking explains the fast improvement in the new programs that make the codes, offering a better security to the system with more efficiency. The expression cracker also belongs to the same field; it makes use of the hacking skills for the unlawful purposes like email id, intruding into other system. Hacking has different types such as backdoor hacking, viruses and worms, Trojan horses, denial-of-service attack, anarchists, crackers, kiddies and ethical hacking [1].

Hyper-jacking attack controls on a hypervisor to compromise the instance VMs. As a consequence of this kind of attack, the hacker takes over the management and control of the guest operating within VM environment; virtualization server and the host OS will be stilled active and in use. Traditional security mitigation techniques are not adequate because the security measures on the guest VMs or sever do not know that host operating system itself has been compromised. If hyper-jacking is achieved by an attacker, he needs to have a processor that can do hardware-assisted virtualization to access the host. Attacker may convince the admin or user to install some malicious code to attack the hypervisor.

2.3 Background Theory of Proposed System

2.3.1 Virtualization Concept

In the era of information technology, the fundamental change is happening in cloud computing with virtualization; this means that the combination (mixture) of hardware and software engineering process that creates virtualization and it can run on the same platform with multiple operating systems (Fig. 2.2).

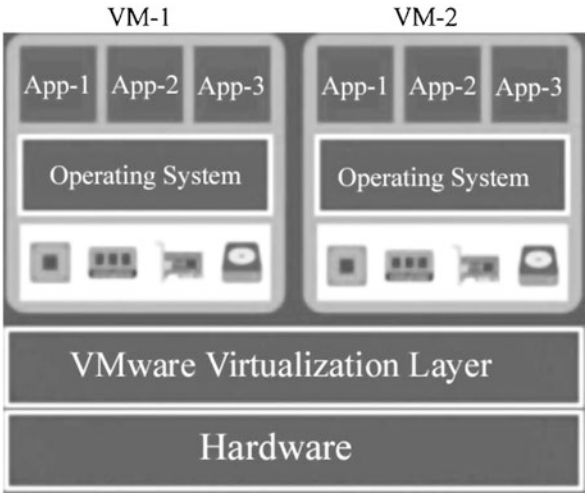

Fig. 2.2 Illustration of layer abstraction in virtualization

Virtualization process becomes critical for business and organization to seek better resource providing, less hardware, easy IT management with economically. But virtualization is a complicated scheme and continually evolves with certain risks concerning hypervisor security. The concept of virtual machine allows the following functions such as isolation, server consolidation, portability, application portability, suspend, and restart.

Based on the data center technology, types of virtualization can be classified below:

- Hardware virtualization
- Network virtualization
- Storage virtualization
- Server virtualization
- Operating system virtualization
- Desktop virtualization
- Application virtualization [6]

2.3.2 Detection Method Based on Behavior Approach

Detection method based on behavior technique only depends on the system activity, and it can be categorized into two parts: the system with hypervisor and system that starved off a hypervisor. There are three kinds of detection method based on behavior technique shown in (Fig. 2.3). Translation look aside buffer TLB-based detection and methods based on errors in hypervisors and errors in CPUs [7].

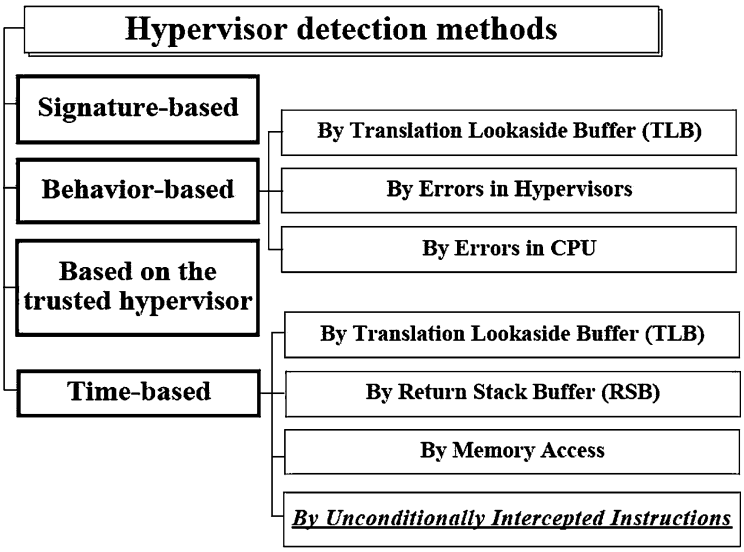

Fig. 2.3 Classification of hypervisor detection methods

2.3.2.1 Translation Lookaside Buffer TLB-Based Approach

Translation lookaside buffer detection approach is likely to be applied at caching memory that stored and used to get more address translation speed to sense a hypervisor [1].

Translation lookaside buffer detection approach includes a set of virtual and physical address; it may be recently accessible to the system. Whenever the operating system has to get access to the memory, translation lookaside buffer entry is looking for this corresponding address. If needed, requested virtual address is exist in the Translation Lookaside Buffer, they saved and retrieved physical address to contact memory.

VM exit guide shows the translation lookaside buffer when a hypervisor is present. On the other hand, without hypervisor, such permission and authorization cannot occur. This is because detection hypervisor reduced checking translation lookaside buffer approach content; this can be done by numerous alternate behaviors, for example, by editing or modifying page table entry (Myers and Youndt 2007) [3].

But, translation lookaside buffer detection approach does not work on central processing units of AMD and other Intel central processing units. The new extra additional translation lookaside buffer fields ASID and process-context identifier will not allow VM exit (virtual machine exit) flush level translation lookaside buffer (TLB) [3].

2.3.2.2 CPU-Based Detection Approach

By using the help of bugs and some instructions in convinced central processing unit model, a hypervisor can be detected whether it (rootkit) is present or not. Other kind of bugs like VMSAVE 0x67 that also freezes the system too. The prefix run time and execution of the VMSAVE 0x67 can halt the virtualization system. These error and bugs occur with hypervisor. If without hypervisor, this kind of error cannot occur (Barbosa 2007). This detection method can be found and applicable in obsolete central processing unit and requires nontrivial adaptation to new central processing units [3].

2.3.3 Hypervisor Model

Hypervisor is a software that distributes and shares computer resources (for instance, processing power unit, random access memory, storage, etc.) in virtual machines, which can be communicated to other computers in the network. It creates virtualization layer that makes server virtualization possible and offers people to share resources. So, the users have to run applications without heavily relying on powerful desktop computers that are costly. Moreover, system administrators can

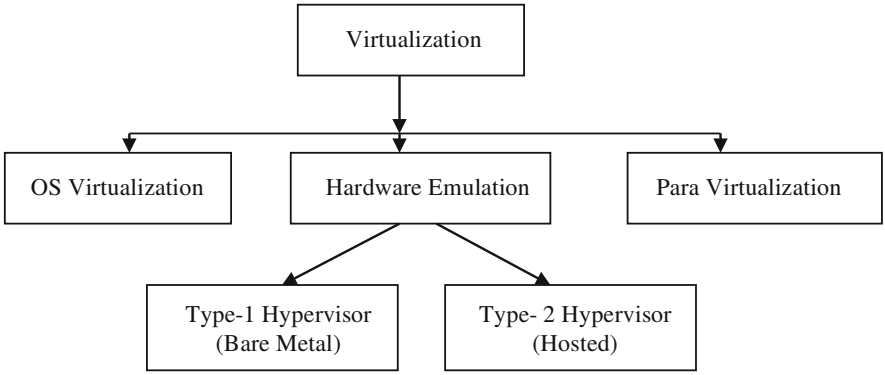

Fig. 2.4 Types of virtualization design chart

also use the hypervisor to monitor and manage VMs with Virtual Machine Manager (VMM). There are two types of hypervisors, and the following are some examples of hypervisors [1] (Fig. 2.4):

- VMware ESX/ESXi
- Hyper-V
- VMware Workstation
- Oracle Virtual-box
- Fusion
- Virtual Server
- Xen Server

2.3.3.1 OS Virtualization

According to Vangie Beal [8] assumption, operating system virtualization refers to the use of software by allowing system hardware to run multiple instances; operating system lets the users to execute different applications.

2.3.3.2 Hardware Emulation

Hardware emulation is generally used to debug, fix, check, and verify a system under enterprise design plan. An administrator has to use hardware emulation if he needs to run an unsupported operating system (OS) within a virtual machine (VM). In such a scenario, the virtual machine does not have direct access to server hardware [9]. Nowadays, virtualization technology can available both free or commercial use. For instance, VMware ESXi, VMware VMs server, Microsoft virtual server, and Xen Server.

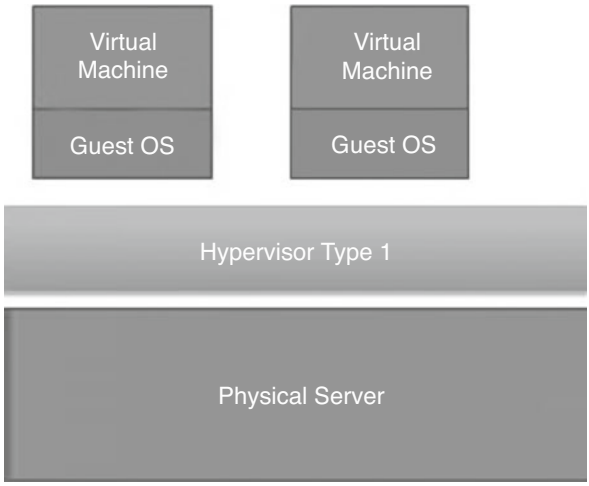

Fig. 2.5 Example demonstration of type 1 hypervisor model

Type 1 Hypervisor

Type 1 hypervisor is loaded directly to hardware; Fig. 2.5 shows the type 1 hypervisor and the following are the kinds of type 1 hypervisors (Fig. 2.6):

- VMware ESX/ESXi for VMware vSphere
- Hyper-V for Microsoft
- Xen Server

Type 2 Hypervisor

On the other hand, type 2 hypervisor is loaded in an operating system running on the hardware that is our laptop or desktop, for example (Fig. 2.7):

- VMware workstation
- Oracle Virtual-box
- Virtual Server
- Fusion for Mac OS

2.3.3.3 Para-Virtualization

Para Virtualization is more complex than hardware emulation technique that mentioned above. It multiplexes access and administrates to hardware infrastructure resources, offering great performance and requiring guest OS modification before deployment, for example, Xen (open source) [8].

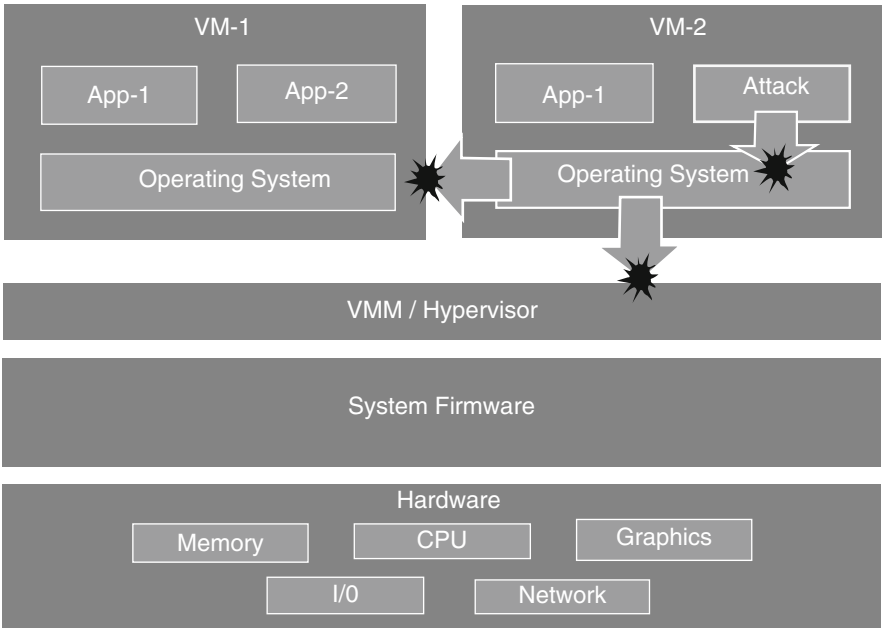

Fig. 2.6 Stack of bare metal hypervisor attack

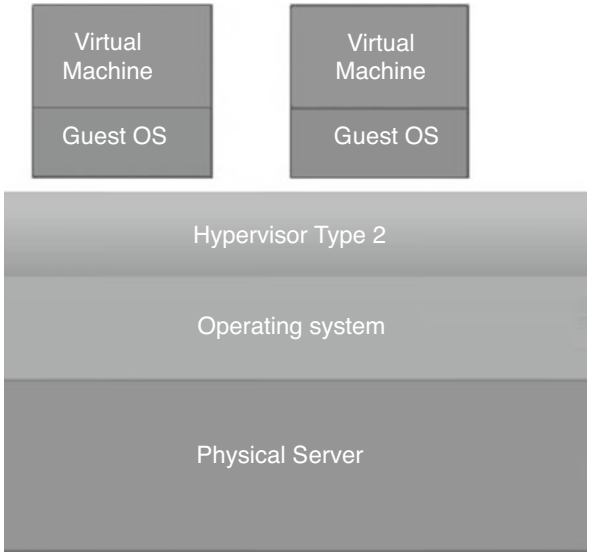

Fig. 2.7 Example demonstration of type 2 hypervisor model

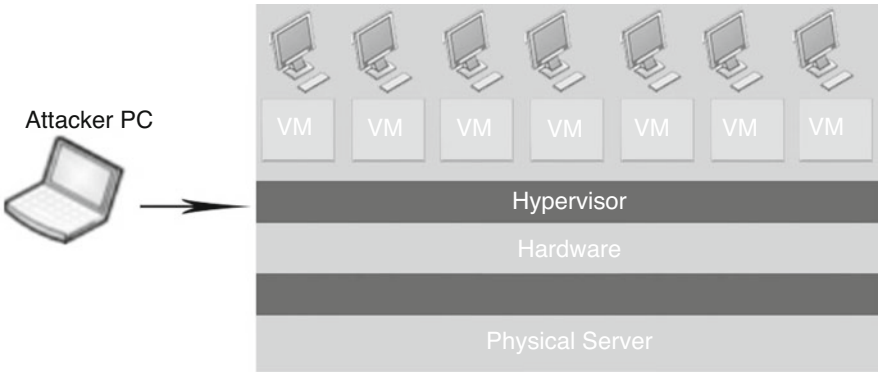

Fig. 2.8 Hyper-jacking attack model

2.3.4 Hypervisor Hijacking Thread Types

Hyper-jacking is a kind of attacking in the place where a hacker takes malicious control over the hypervisor that creates the virtual environment within a virtual machine (VM) host. The idea of that attack is to target the operating system that is below that of the virtual machines so that the attacker's program can run and the applications on the VMs above it will be completely oblivious to its presence [10] (Fig. 2.8).

Hyper-jacking includes installing a malicious activity, fake hypervisor can manage and control to accomplish the entire server system. Regular security measurements are ineffective to secure the system because the operating system is not aware that the machine has been compromised. In hyper-jacking, the hypervisor mainly works in stealth mode is to run under the virtual machine; it is more difficult to detect and more likely gain access to computer servers which affect the operation of the entire institution, company, or business organization. If the hacker gains access to the hypervisor, everything that is connected to that server can be manipulated. The hypervisor represents a single point of failure when it comes to the security and protection of sensitive information. For a hyper-jacking attack to be completely successful, a hacker will have to take control of the hypervisor by the following methods:

- By injecting a rogue hypervisor under the original hypervisor
- By using direct control of the primary hypervisor
- By attacking rogue hypervisor on top of an existing hypervisor definition concept

Hypervisor vulnerability is defined that if hackers manage and achieve to compromise hypervisor software, they will release access to every VM and the data stored on them. While hypervisors are overall well-protected and robust (strong), security specialists can say that hackers will finally discover a bug in the software like a zero-day attack.

Currently, Reports of hypervisor hijacking attacks are very rare and limited; but in concept assumption, cybercriminals can run a program that breaks out of a VM and has direct interaction to the hypervisor. From this step, they can control everything, from access privileges to computing resources. There are three types of hypervisor threats:

- Internal threats
- Technology threats
- External threats

The VMs and hypervisor allocate as a distributed nature. So, another point of weakness in vulnerability is the network. Since hypervisors distribute VMs via the business organization network, they can be susceptible to remove intrusions and denial-of-service attacks if we don't have the right protections in that position. These are some types of common attack vectors [11].

- Virtual CPUs
- Software memory management units
- Interrupting and timer mechanisms
- Input and output (I/O) and networking
- Virtual network layer (e.g., vSwitch)
- System calls or hypercalls
- Hypervisor add-ons or extension

These are some recently happened threats types:

- Vulnerability from outdated operating system and lack of active patching
- Poor network performance (every VM can have a resource cost)
- Intel disclosed Spectre-like L1TF vulnerabilities, August 17, 2018
- Hardware debug documentation leads to widespread vulnerability, May 11, 2018
- AMD patches in testing with ecosystem partners, May 04, 2018 (Fig. 2.9)

In any fields of the system, there are pros and cons, opportunities and challenges. In virtualization technology, it has many aspects of IT management, but the nature of virtualization may also have complicated task of cyber security control in a new threat vector point of view.

2.4 Serious Vulnerabilities in Virtualization

The following sections are phenomena of risk of virtualization that occur when the number of virtual machines on a network reaches a place where the administrator cannot control and manage these VMs effectively. The session shows some attacks with virtual machine and their serious, critical vulnerabilities and so on.

VM architecture and setting are variations of common threats such as denial-of-service attacks, session hijacking attack, DNS hijacking attack, others still hugely

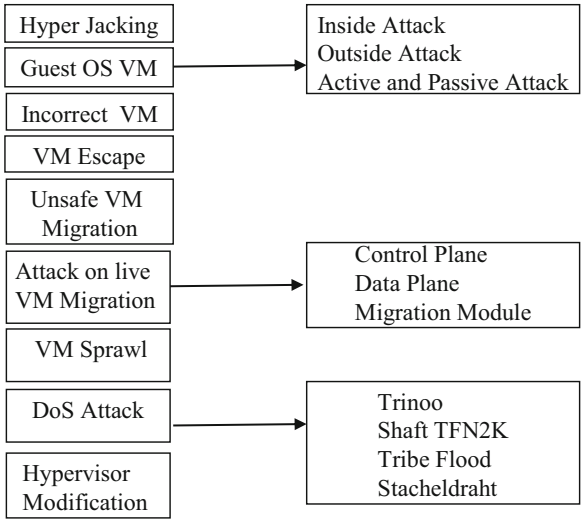

Fig. 2.9 Taxonomy of virtual machine vulnerability to persuade threat

exist as a theoretical but are likely approaching as buzz and means increase. That kind of critical weaknesses are discussed as follows.

2.4.1 VM Sprawl

Virtualization technology is not only improves hardware efficiency but also reduces time and cost. VM sprawl is one of the biggest issues that facing many business organizations using desktop and server virtualization. VM sprawl can occur many VMs on a network where administrator lost control on his virtual machine. Attackers can get opportunities because of lack of systematic monitoring resources [12].

2.4.2 Hyper-jacking Attack

Hypervisors are hijacked to gain access and control of VMs and its data. Hyper-jacking attacks can occur both type 1 and type 2 hypervisor. Although type 2 hypervisors run over a host OS, type 2 hypervisors can be regarded as a theoretical approach because this type of hyper-jacking is very rarely found in real-world virtualization environment due to difficulty of direct access to hypervisor. However, this type of attack can be considered as a real threat, and administrator should plan and prepare for it as an offensive nature [13].

2.4.3 VM Escape Method

In order to get direct access to the hypervisor, guest operating system escapes from their VM encapsulation. This kind of opportunity gives the attacker for all access to VMs, if guest and host privileges are high. This kind of attack is also not well-known by all attackers, but administrators and experts have to consider VM escape as the most serious threats in VM security [13].

2.4.4 Denial-of-Service Attack

An attempt to deprive victim's resource to make unavailable for authorized users by shutting down the services. The attackers targeted different resources such as network resources (data store, CPU and servers) [13].

2.4.5 Incorrect VM Isolation

VM isolation has an important role to make virtualized environment safe. For secure and right sharing resources, VMs have to be isolated from each other. When communication between one VM to another VM, they should be restricted just like a traditional physical machine with physical firewall. On the other hand, because of the poor control and security policies, it can lead to the isolation breaches in VMs. Attackers can exploit and cause incorrect VM isolation which can reduce the VM performance [13].

2.4.6 Unsecured VM Migration or VMotion

This kind of event occurs when VM migrated to a new host machine with lack of security policies and configuration updated. Then, host and other guest operating systems are more vulnerable, and attackers can get more chance to attack because of no awareness of system's weaknesses, vulnerabilities, and alerts by system administrators [13].

2.4.7 Host and Guest Vulnerabilities

Because of multiple weaknesses of windows and operating system, some host and guest communications have several system vulnerabilities in virtualization

environment. Similar to that, other systems can lead to vulnerabilities such as in email, web browsing, and network protocol. But co-hosting and virtual linkages can make serious attack and cause VM damaging effect [13].

2.5 Hacker Lifestyle

The act of accessing computer system and network without authorization is called hacking. The person who conducts this activity is referred to as hackers. The attacker will conduct many preattack activities in order to obtain information successfully. Frequently, they can alter or change or modify security systems for the success of hacker's business goal; it can differ from the actual purpose of the system [1]. Nowadays, many organizations hire hackers as their staff to find system flaws, weakness of organization, and vulnerable areas to be a good security system or organization and prevent malicious hackers who are breaking into the system [1].

2.5.1 White Hat Hacker

White hat hackers are good person and also referred to as an ethical hacker. They are working with organizations to harden the security system and to get more profit for the organization. A white hat hacker legally has permission to exploit the targeted system of the organization and compromise or tested machines within the prescribed rules or setting in advanced rules of engagement. Individual hacker specializes in and analyzed ethical hacking tools, techniques, and methodologies to secure an organization's information systems [1].

Not having the same function of the black hat hacker does, ethical hackers have to exploit security network flaws and look for backdoors when they are legally permitted to do so and get an authority. This kind of hackers always tries to disclose every vulnerability they find in the company's security system so that it can be fixed before they are being exploited by malicious actors [1].

2.5.2 Black Hat Hacker

The meaning of black hat originated and came from Western movies, where the bad guys wore black hats and the good guys wore white hats [1].

A black hat hacker is an individual person who attempts to gain unauthorized entry into a system or network to exploit the organization's information for malicious reasons. The black hat hacker does not have any permission or authority to compromise their targets. They try to inflict damage by compromising security

systems, altering functions of websites and networks, or shutting down systems. They often do so to steal or gain access to passwords, financial information, and other personal data [1].

2.5.3 Gray Hat Hacker

Grey hat hacker exploits networks and computer systems in the way like a black hat hacker does. They do not intend to do any malicious activity like black hat hacker, disclosing all loopholes and vulnerabilities to law enforcement agencies or intelligence agencies. Usually, grey hat hackers hack into computer systems to notify the administrator or the owner that their system/network contains one or more vulnerabilities in order to be fixed immediately. Grey hats hacker may also extort the hacked, offering to correct the defect for a minimal cost [1].

2.6 Cyber-Attack Lifecycle

The characteristic of cyber-attack lifecycle can be categorized as follows:

2.6.1 Phase 1: Reconnaissance

This is the initial step of information gathering stage. Attacker collects targeted organization's information as possible as he can via several ways in order to satisfy the goal of the attackers such as financial gain, intentional brand damage, and accessing sensitive information [14].

2.6.2 Phase 2: Initial Compromise

After reconnaissance stage, the next step is initial compromise phase. In this stage, attackers break out the system, gaining access to the internal network via bypassing the defended perimeter (Firewall). Sometimes, hacker used by compromising user account or system. Attacker always used to deceive the victim with phishing email or spear phishing attack. Once the victim's machine gets an email in their mail inbox and attachment is opened, this suddenly generated malware is controlled by the attacker. This stage can get benefit for attacker to get further instructions such as lateral movement [14].

2.6.3 Phase 3: Establish Foothold

After phase 2 stage, this phase immediately followed the initial compromise step. Typically, this phase 3 involves the attacker downloading some malicious software in order to establish command and control and persistent, long-term, remote access to victim's machine [14].

2.6.4 Phase 4: Lateral Movement

After being connected and gaining access to the internal network, attacker uses lateral movement to look for another additional system to compromise user account, privilege level. Attackers use this technique to go further step through the network when they search for the organization's key data and assets [14].

2.6.5 Phase 5: Target Attainment

After the malicious software activities have established at a lateral movement connection with multiple machines in the network, another step will be carried out for unsolicited authorization, account compromising, and privilege escalation [14].

2.6.6 Phase 6: Ex-filtration, Corruption, and Disruption

This is the final phase of attack, the permission escalated are used to transmit data whole of the network, it is called ex-filtration [14]. They steal sensitive information from the business organization and corrupted critical information resources including delete file and disruption.

2.6.7 Phase 7: Malicious Activities (Fig. 2.10)

Normally, threat lifecycle in cloud computing is the same as the traditional network environment.

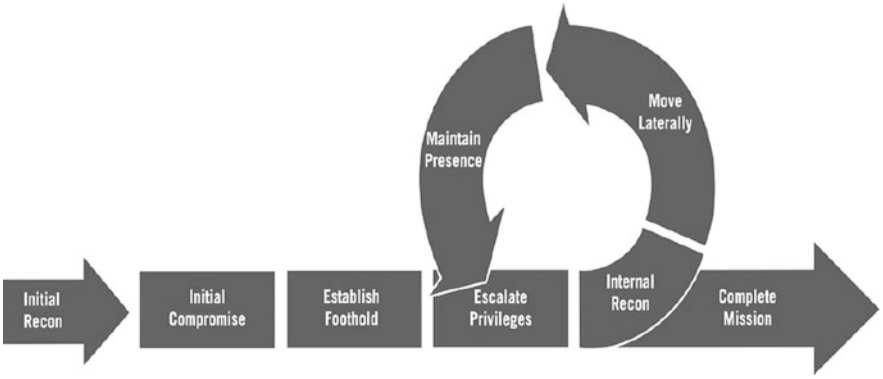

Fig. 2.10 Hacker attack life cycle

Table 2.1 IP addresses domain of experimental lab

No	FQDN	IP address	System	Installations
1	vcenter.domain1.site	172.16.10.1	Windows 2012 R2	DNS, DHCP, NAT, NTP, and VMware vCenter Server
2	esx1.domain1.site	172.16.10.11	VMware ESX	ESXi 5.0
3	esx2.domain1.site	172.16.10.12	VMware ESX	ESXi 5.0
4	nas1 .domam1, site	172.16.10.21	NAS	Openfiler
5	research.domain1. site	DHCP	Windows XP (Management PC)	VMware vSphere Client

2.7 Implementation Framework for Protecting Mechanism

2.7.1 VM Creation of Virtual Network Configuration

In this experiment, the system tested both type 1 and type 2 hypervisor attack on hypervisor hijacking attack.

As first step of proposed system design, a virtual environment was created for both type 1 and type 2, and the networks were configured on the host server machine, with one network allowing access to the Internet and an internal one with the IP address range shown in Table 2.1 and Fig. 2.14 as IP address domains. For type 2 hypervisor, 10.0.0.0/24 is used to communicate between the virtual machines. Then, the Management VM was created with Linux open-source software through a desktop environment installed, before the network interfaces were configured and SSH (Secure Socket Shell) access was enabled for remote access.

The next step is the creation of the basic VM template which was used to create a total of three VMs for the internal network by installing their respective servers one by one (Figs. 2.11 and 2.12).

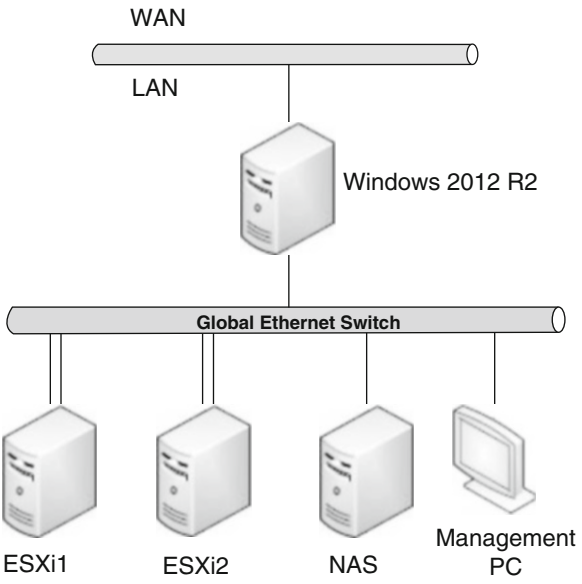

Fig. 2.11 Configuration of virtual machine in experimental lab

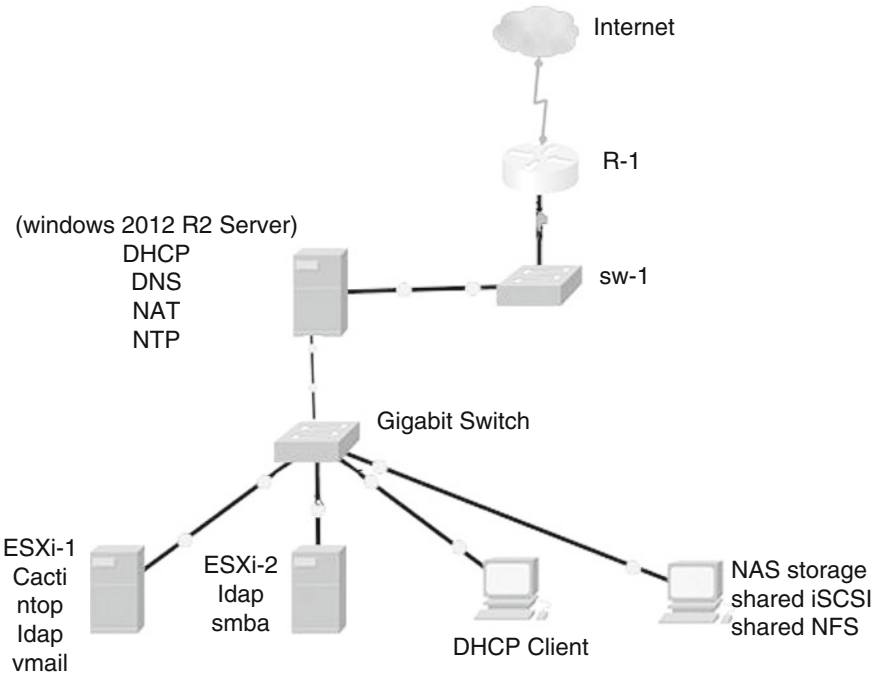

Fig. 2.12 Configuration of virtual machine in tested system of type 1 hypervisor

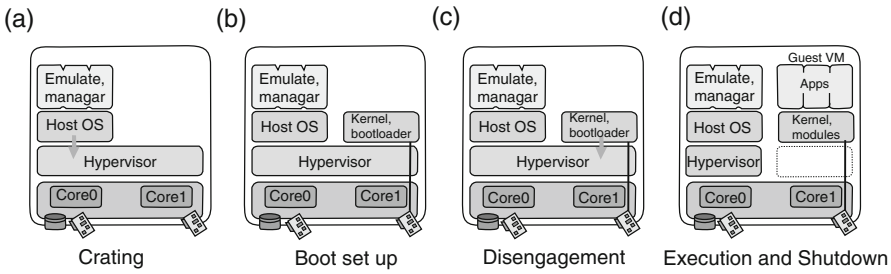

Fig. 2.13 Configuration bridging of virtual machine in type 1 hypervisor

During the setup, the following stages are configured:

- Free version of hypervisor to manage the virtual machine
- Required to navigate each hypervisor to monitor for attackers
- Configuring the pre-allocation of processor cores and memory resources
- Using virtualized I/O devices to apply services
- Monitoring modifications to the guest OS to perform all system discovery during boot setup
- Setting up (NIC) card for the guest virtual machine in more direct contact with the underlying hardware (Figs. 2.13, 2.14, 2.15, and 2.16)

2.7.2 Tested Methodology

In VM preparation for type 2

Step 1: Kali Linux is configured as main attacking platform.
Step 2: In virtual box configuration, change Kali network NIC for NAT mode to Bridge.
Step 3: Setting login password with username = root, password = root.
Step 4: Open terminal window and type ifconfig command.

The IP address of Kali Linux will show 10.0.0.12/24.

The system used the following steps to achieve successful VM configuration. After the package installation process, it can use the following commands.

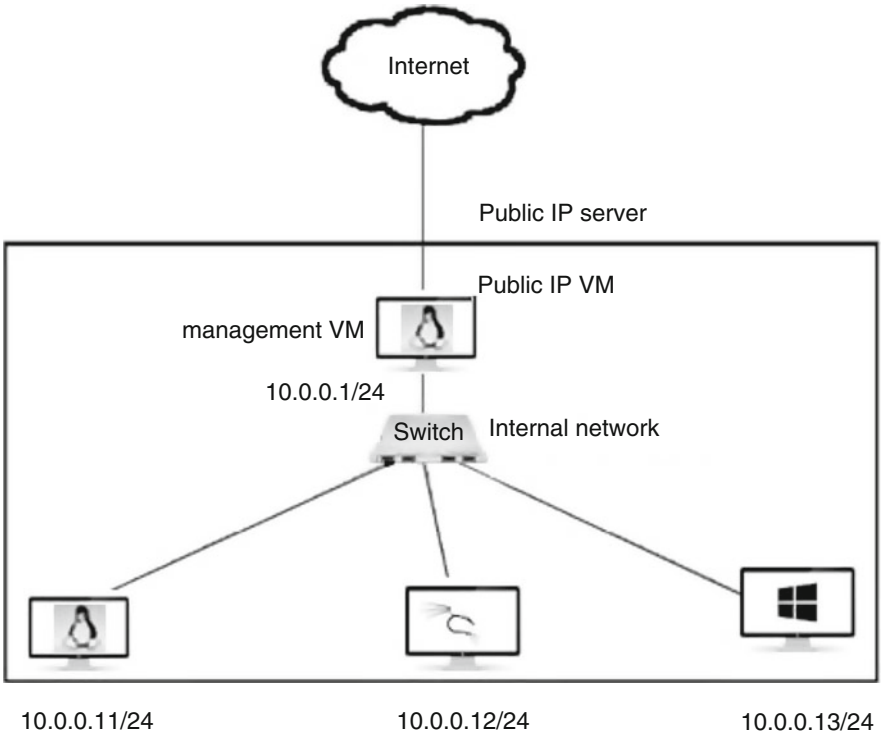

Fig. 2.14 Tested in type 1 hypervisor environment of virtual machine

```
[    0.000000] Initializing cgroup subsys cpu
[    0.000000] Initializing cgroup subsys cpuacct
[    0.000000] Linux version 3.13.0-24-generic (buildd@panlong) (gcc version 4.8.2 (Ubuntu 4.8.2-19u
-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 (Ubuntu 3.13.0-24.46-generic 3.13.9)
[    0.000000] Command line: BOOT_IMAGE=/boot/vmlinuz-3.13.0-24-generic root=UUID=05088af6-6cef-4516
2ea0a ro
[    0.000000] KERNEL supported cpus:
[    0.000000]   Intel GenuineIntel
[    0.000000]   AMD AuthenticAMD
[    0.000000]   Centaur CentaurHauls
[    0.000000] e820: BIOS-provided physical RAM map:
[    0.000000] BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
[    0.000000] BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000000100000-0x000000007fffdfff] usable
[    0.000000] BIOS-e820: [mem 0x000000007fffe000-0x000000007fffffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000feffc000-0x00000000feffffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
[    0.000000] NX (Execute Disable) protection: active
[    0.000000] SMBIOS 2.4 present.
[    0.000000] DMI: QEMU Standard PC (i440FX + PIIX, 1996), BIOS Bochs 01/01/2011
[    0.000000] Hypervisor detected: KVM
[    0.000000] e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
[    0.000000] e820: remove [mem 0x000a0000-0x000fffff] usable
[    0.000000] No AGP bridge found
```

Fig. 2.15 Command line tested to show hypervisor type

Fig. 2.16 Perl script of command line in detail

```
#!/bin/bash -
# virt-what.  Generated from virt-what.in by configure.
# Copyright (C) 2008-2011 Red Hat Inc.
# Do not allow unset variables, and set defaults.
set -u
root=''
skip_qemu_kvm=false

VERSION="1.13"

function fail {
    echo "virt-what: $1" >&2
    exit 1
}

function usage {
    echo "virt-what [options]"
    echo "Options:"
    echo "  --help          Display this help"
    echo "  --version       Display version and exit"
    exit 0
}

# Handle the command line arguments, if any.

TEMP=$(getopt -o v --long help --long version --long test-root: -n 'virt-wha
if [ $? != 0 ]; then exit 1; fi
eval set -- "$TEMP"

while true; do
    case "$1" in
        --help) usage ;;
        --test-root)
            # Deliberately undocumented: used for 'make check'.
            root="$2"
            shift 2
```

Step 1: #service libvirtd start
Step 2: #chkconfig libvirtd on
Step 3: #systemctl enable libvirtd.service
Step 4: #virsh list
Step 5: #mkdir -p /home/vmsserver-FM
Step 6: [root@server] # virsh
Step 7: virsh # help
Step 8: virsh # list –all
Step 9: virsh #dominfo server-VM
Step 10: virsh # start server-VM
Step 11: virsh # shutdown server-VM

Many virtualization implementations run on Linux system (some also can run windows). Some are quite easier to set up and manage than other kind of implementation method. In this section, the system tested both high-level virtualization and common virtualization concepts as a type 1 (bare metal) hypervisor and type 2 (hosted) hypervisor.

2.8 Behavior-Based Analysis for Hypervisor Detection

Intrusion detection systems (IDSs) have a vital role for infrastructure security in cloud computing which are designed to detect log and incident response for using

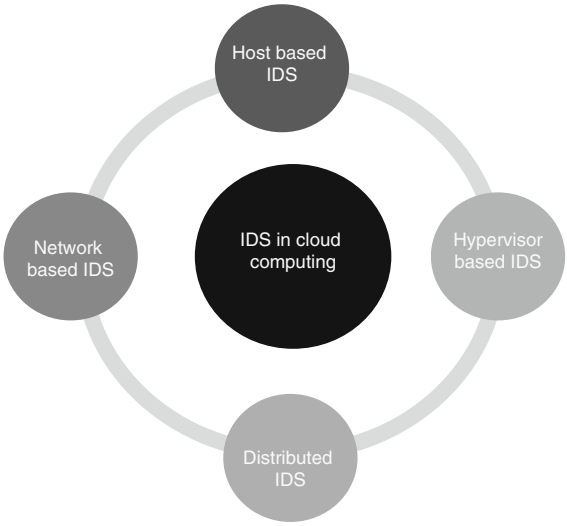

Fig. 2.17 Cloud-based intrusion detection system

unauthorized behavior both in real time and after the event. In cloud computing, there are four types of IDSs systems such as network-based IDS, host-based IDS, hypervisor-based IDS, and distributed IDS as shown in Fig. 2.17.

Behavior-based detection approach is a proactive approach method to manage security incidents that include monitoring and see log process for abnormal behavior of users, devices, network, and servers in order to block (stop) suspicious events. This model depends on a collection set of normal behavior like users and traffics. If the activities or pattern is considered as abnormal, the system is regarded as suspicious (malicious) activities. Behavior-based detection approach analyzes data and application based on unknown attacks. On other side, knowledge-based technique is used known attack. For unknown attack, there can be high false positive rates; any new traffic pattern can be regarded as suspicious. This model can detect zero-day attack (Table 2.2).

2.9 Protecting and Mitigation Technique for System Hardening

The major important primary technique for secure hypervisor is to keep separate from usual traffic. The access to guest operating system should be defined by restricting the access to the hypervisors with the intention of avoiding hyper-jacking attacks (Tables 2.3, 2.4, and 2.5).

Table 2.2 Analysis of cloud-based detection system

Type of IDS	Features	Limitations/challenges	Position in cloud	Deployment and monitoring
Host-based IDS	Identify intrusions by monitoring system activity (Logs, Files system, etc.)	It must be installed on each machine (VM, hypervisor, host). Monitors the machine where it is deployed	In each virtual machine, in hypervisor, or in host machine	In VMs: cloud user. In hypervisor or in a host machine: cloud provider
Network-based IDS	Identify intrusions by monitoring network traffics	Difficulties of detecting intrusions in a virtual network. Can only detect intrusions coming from the network where it is deployed	In an external or virtual network	Cloud provider
Hypervisor-based IDS	Monitor and analyze communication between VMs, between hypervisor and VMs and between hypervisor and virtual network. It is the most suitable for cloud	Resources on the subject are limited. Difficult to understand	In hypervisor	Cloud provider
Distributed IDS	It allows a company to efficiently manage its incident analysis resources and to identify threats to the network across multiple network segments	The adoption of DIDS is still challenging due to the complex architecture of the infrastructure and the distinct kinds of users lead to different requirements and possibilities for being secured	It operates both on host and network	Cloud provider

Table 2.3 Analysis of hyper-jacking attack and mitigation technique

Attack mechanism	Mitigation technique
DoS Attack	Disable IP broadcast Disable unused services Deploy firewall rules Deploy IDS policy and rules Apply security patches on host
Live VM migration	Encryption of data by the hypervisor Use IPsec tunnel Source virtual machine monitor level virtual firewall Destination virtual machine monitor level virtual firewall
Hyper-jacking	Separate traffic from usual traffic Restrict the access Regular patches
VM escape	Should be provided access based on role Host should run only the required resource-sharing functionalities/services Guest OS should run less number of application to avoid any pen test
VM sprawl	Restrict the access Should be provided access based on role Should be made periodic verification Properly turn off identified idle VM
Guest OS vulnerabilities	Periodically perform the patching process Adopt firewall applications and traffic Really needed applications should be installed
Hyper-wall	Combination of another model for more security Confidentiality and integrity protection Multi-facilitated functions compared with others

Table 2.4 shows some integrity of virtual machine monitoring security techniques

Tools	Description
Hyper-safe	The lightweight approach of hypervisor for controlling flow of integrity check to provide lifetime
Hyper-sentry	To provide stealthy and in context measurement for precisely measuring integrity System management mode weakness and limitation, NOVA appears

Table 2.5 shows control flow integrity of virtual machine

Tools	Description for mitigation
Non-bypassable memory lockdown	Endue VMM with self-protection Protect memory page and attribute from malicious modification
Restricted pointer Indexing	Memory page and control data protection

2.10 Future Studies

Going forward for future research, this paper will discuss in more detail measurement of security that yields comparison results to take achievement in more virtualized implementations to meet the needs of current customer issues and requirements.

2.11 Conclusion

In this proposed system, a very recent and fresh comprehensive survey on virtualization threats and vulnerabilities is presented with the classification of hypervisor hijacking attacks with existing defense mechanisms. The purpose of this paper is introducing the approach that intended to harden and protect the business and organization's values in the virtualization environment which is mostly used in modern cloud architecture. The system tested both type 1 and type 2 hypervisors. Actually, there is a very rare report of type 1 hypervisor hacks, but according to the theoretical assumption, any cybercriminal can run a program and break down the system of virtual machine. So as an administrator's point of view, he/she should be prepared for this kind of attack as an offensive nature. So, hardening hypervisor hijacking attack on the virtual reality is an actual successful proof of concept as a real-world threat. Although virtualization threats and attacks are listed and categorized in this paper, luckily, high impact hypervisor attack on virtualization can be avoided by using behavior-based detecting method. Most of the motivation and methods of traditional threats and attacks are basically the same in VM environment. So, administrators may have to encounter and face with similar attack technique. Anyway, security is very long and hard process to protect the organization, for all layers to harden.

References

1. http://www.ukessays.com/
2. https://www.zdnet.com/article/detecting-the-blue-pill-hypervisor-rootkit-is-possible-but-not-trivial/
3. D. Morabito, Detecting hardware-assisted hypervisor rootkits within nested virtualized environments. Master's thesis, AFIT/GCO/ENG/12-20, WrightPatterson Air Force Base, OH, USA, Accession Number ADA563168, June 2012
4. J. Rutkowska, Subverting VistaTM kernel for fun and profit, http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Rutkowska.pdf
5. D.D. Zovi, Hardware virtualization rootkits, http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Zovi.pdf
6. D. Ruest, N. Ruest, *Virtualization: A Beginner's Guide* (McGrawHill Publication, New York, 2009), p. 25

7. I. Korkin, Two challenges of stealthy hypervisors detection: Time cheating and data fluctuations. J. Digit. Forensic Secur. Law
8. https://www.webopedia.com/TERM/O/operating_system_virtualization.html
9. https://searchservervirtualization.techtarget.com/definition/hardware-emulation
10. http://www.wikipedia.com
11. A.M. Azab, P. Ning, Z. Wang, X. Jiang, X. Zhang, N. C. Skalsky, HyperSentry: Enabling stealthy in-context measurement of hypervisor integrity. Proceedings of the 17th ACM Conference on Computer and Communications Security CCS, 2010, pp. 38–49
12. M. Ali, S.U. Khan, A.V. Vasilakos, Security in cloud computing: Opportunities and challenges. Inf. Sci. **305**, 357–383 (2015)
13. https://pentestlab.blog
14. https://www.helpnetsecurity.com/2017/03/06/cyber-attack-lifecycle/