SECURING VIRTUALIZATION: TO MITIGATE TCP-DDOS BETWEEN MULTIPLE TENANTS ON THE SAME PHYSICAL HOST IN CLOUD COMPUTING

Dissertation Submitted to the Central University of Punjab

For the award of

Master of Technology

In

Computer Science & Technology

By

Kanika

Supervisor

Er. Navjot Sidhu

Centre for Computer Science & Technology

School of Engineering & Technology

Central University of Punjab, Bathinda

September, 2014

DECLARTION

I declare that the dissertation entitled "SECURING VIRTUALIZATION: TO MITIGATE TCP-DDOS BETWEEN MULTIPLE TENANTS ON THE SAME PHYSICAL HOST IN CLOUD COMPUTING" has been prepared by me under the guidance of Er. Navjot Sidhu, Assistant Professor, Centre for Computer Science and Technology, School of Engineering and Technology, Central University of Punjab.

No part of this dissertation has formed the basis for the award of any degree or fellowship previously.

Kanika

Centre for Computer Science and Technology,

School of Engineering and Technology,

Central University of Punjab, Bathinda - 151001.

Date:

CERTIFICATE

I certify that Kanika has prepared her dissertation entitled "SECURING VIRTUALIZATION: TO MITIGATE TCP-DDOS BETWEEN MULTIPLE TENANTS ON THE SAME PHYSICAL HOST IN CLOUD COMPUTING", for the award of M.Tech. degree of the Central University of Punjab, under my guidance. She has carried out this work at the Centre for Computer Science and Technology, School of Engineering and Technology, Central University of Punjab.

Er. Navjot Sidhu

Assistant Professor

Centre for Computer Science and Technology,

School of Engineering and Technology,

Central University of Punjab, Bathinda - 151001.

Date:

ABSTRACT

Securing Virtualization: To mitigate TCP-DDOS between Multiple Tenants on the same Physical host in Cloud Computing

Name of student: Kanika

Registration number: CUPB/MTECH/SET/CST/2012-13/06

Degree for which submitted: M.Tech.

Name of supervisor: Er. Navjot Sidhu

Name of centre: Centre for Computer Science and Technology

Name of school: School of Engineering and Technology

Key words: Cloud Computing, Multi-tenancy, Virtualization, Hypervisor, Network Security, DDoS Attack.

Cloud computing is the fastest growing technology in the IT world. The technology offers reduced IT costs and provides on the demand services to the individual users as well as organizations over the Internet. The means of cloud computing is obtained by the virtualization of the resources such as hardware, platform, operating system and storage devices. Virtualization permits multiple operating systems to run on the same physical machine. Multiple tenants are unaware of the presence of the other tenant with whom they are sharing the resources. The co-existence of multiple virtual machines can be exploited to gain the access over other tenant's data or attack to deny of services. The significant concern is insuring the security and providing isolation between multiple operating systems. Denial-of-Service (DoS) attack poses a serious network security challenge to the virtualized cloud computing. All the virtual machines and the host machine shares common resources over the cloud computing. A malicious virtual machine can exhaust the common resources by flooding the co-existing VM with high rate of unreasonable network traffic. The threat of DoS attack becomes even more severe with DDoS (Distributed Denial-of-Service) attack. Other virtual machines are compromised on the virtualized cloud to perform DDoS attack.

The dissertation aims to provide an analysis of the different attacks raised by the multi-tenancy and the virtualization in an IaaS cloud. The research focuses on the threats arises from malicious tenants to the co-existing tenants on the same physical host. As part of the aim of this research, the terms of cloud computing, multi-tenancy and virtualization are analysed. The vulnerability of the DDoS attack by a malicious virtual machine over co-existing virtual machine in the private cloud infrastructure is explored along with a mechanism on how to approach it. The research approaches to provide a security model to mitigate the effect of denial of service attack from the virtualized cloud computing.

(Kanika) (Er.Navjot Sidhu)

DEDICATED TO GOD,
MY LOVING FAMILY MEMBERS AND MY FRIENDS

ACKNOWLEDGEMENTS

First of all, I am extremely grateful to my research guide, Er. Navjot Sidhu, Assistant Professor, Centre for Computer Science and Technology, for her valuable guidance, scholarly inputs and consistent encouragement, I received throughout the research work. This feat was possible only because of the unconditional support provided by Ma'am. A person with an amicable and positive disposition, Ma'am has always made her available to clarify my doubts despite her busy schedules and I consider it as a great opportunity to do my research under her guidance. Thank you Ma'am, for all your help and support.

My sincere thanks also go to Er. Surinder Singh Khurana, Assistant Professor, Centre for Computer Science and Technology, for all his support and guidance throughout my research. His support has been invaluable on both an academic and a personal level, for which I am extremely grateful.

I thank Prof. A.K Jain, CoC, Centre for Computer Science & Technology, faculty of Centre for Computer Science & Technology and staff of University Computer Centre for the academic support and the facilities provided to carry out the research work at the university.

My greatest appreciation and friendship goes to my friends, who were always a great support in all my struggles and frustrations in my new life and studies. I could always talk about my problems and excitements to them. Thanks them for questioning me about my ideas, helping me think rationally and even for hearing my problems.

I would like to thank my family, especially my mother and father for always believing in me, for their continuous love and support in my decisions. Without whom I could not have made it here.

(Kanika)

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATIONS

Sr. No.	Full form	Abbreviation
1.	Acknowledgement	ACK
2.	Address Resolution Protocol	ARP
3.	Applications	Apps
4.	Application Programming Interface	API
5.	CPU Central processing Unit	CPU
6.	Distributed denial of service	DDoS
7.	Finish	FIN
8.	Infrastructure as a Service	IaaS
9.	Institute of Electrical and Electronics Engineers	IEEE
10.	Internet Protocol	IP
11.	Media Access Control	MAC
12.	Network Interface Card	NIC
13.	Platform as a Service	PaaS
14.	Software as a Service	SaaS
15.	Synchronization	SYN
16.	Transmission Control Protocol	TCP
17.	VM Virtual Machine	VM

CHAPTER 1
INTRODUCTION

Cloud Computing is the fastest growing technology in the IT world with the support of Internet network infrastructure. By using cloud computing services an organization, a company or even a private person can make use of resources, i.e. hardware and software over the Internet to develop or maintain their data. This chapter includes an introduction to the Cloud Computing. A short description about its characters, services, together with advantages and disadvantages are provided. The concept of Multi-tenancy environments and virtualization technologies along with the challenges raised when used in the cloud are also included in this chapter.

1.1Cloud Computing

Popularity of cloud computing is increasing day by day in the distributed computing environment. There is a growing trend of using cloud environments for storage and data processing needs. Cloud computing is an Internet-based computing, whereby shared resources, software, and information are provided to computers on demand. To use the full potential of cloud computing, data is transferred, processed, retrieved and stored by external cloud providers.

The National Institute of Standards and Technology (NIST) has provided the definition of cloud computing as (Mell & Grance, 2011): *"Cloud computing is a* model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four *deployment models."*

Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. Examples of cloud services include on-line file storage, social networking sites, web-mail and on-line business applications. Cloud computing creates exciting opportunities like reduced costs and flexibility to the users.

Cloud computing is a virtual infrastructure which provides shared information and communication technology services, via an Internet. Cloud computing provides a computer user access to Information Technology services (i.e., applications, infrastructure, data storage) via Internet without any deployment of the infrastructure at the user's site.

Cloud computing hides the complexity and details of the underlying infrastructure from users by providing simple graphical interface or API (Applications Programming Interface).

When an organization decides to move to the cloud, the data is no longer on their hands. It also comprises of some risks like data security within the cloud. That's why it is very important to protect the confidentiality, availability and integrity of the data (Velte, Velte &Elsenpeter, 2009).

1.1.1 Service Models of Cloud Computing

Once a cloud is established, how its cloud computing services are deployed in terms of business models can differ depending on user's requirements. According to (Velte et al., 2009) cloud service providers offer services that are separated into three categories as:

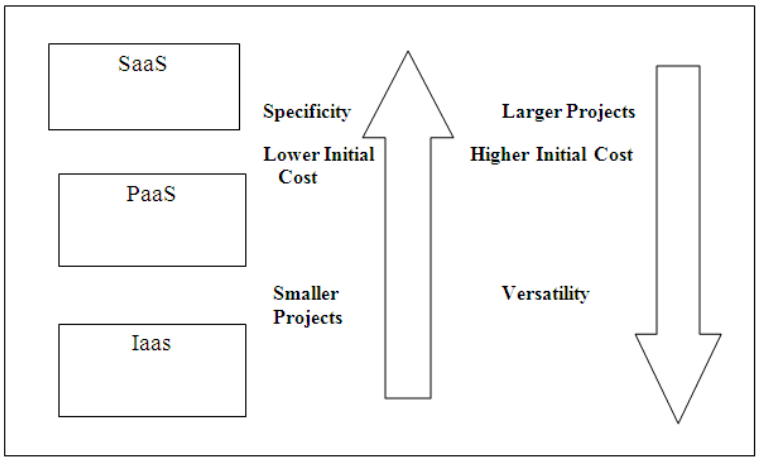

Figure 1.1: Cloud Computing Model

- **Software as a Service (SaaS)**: In the model, software are offered as a service on demand to the customers. Multiple tenants are serviced via running single instance of the service. Customers are billed based on usage and there is no need for investment in servers or software licenses. For the providers, the costs are also lowered, as there is need of single application

to host and maintain. Software as service provided by the companies such as Google, Salesforce, Microsoft, Zoho, etc.

- **Platform as a Service (Paas):** PaaS provides complete platform required to develop user specific applications and services over the Internet. Platform as a service offers a combination of operating system and application servers, such as Linux, Apache, MySql, PHP, etc. PaaS provides the freedom to the user to build their own applications, which run on the cloud service provider's infrastructure. Examples of PaaS include Google App Engine, windows Azure, Force.com, etc.
- **Infrastructure as a Service (Iaas):** IaaS offers complete infrastructure such as servers, basic storage systems, networking equipments over the Internet. Here multiple tenants share a virtualized environment. Tenants are coupled with managed services for the operating system and application support. The users deploy their software on the cloud's infrastructure. IaaS is offered by the organisations such as Amazon, GoGrid, 3 Tera, etc.

1.1.2 Deployment Models in Cloud Computing

As demonstrated in (Mell & Grance, 2011) there are four deployment models of cloud computing. All of these models can be used with any of the service models (SaaS, PaaS or IaaS).

- **Private Cloud:** The cloud infrastructure is built and operated for a particular organization comprising multiple users. The dedicated services of the cloud are only provisioned to the particular organization. It may be owned, managed, and operated by the organization or a third party. Private clouds supported software are Open Stack, Cloud Stack, Virtual Box and VMware ESXi.
- **Community Cloud:** In community cloud, organizations having similar requirements share a common cloud. The cloud is managed by the organizations in the cloud or third party. Eliminating duplicity of same system infrastructure saves time and money as compared to private cloud. For example: Google Apps for Government, Microsoft Government Community Cloud.
- **Public Cloud:** In the public model, services are provided to users by the cloud service provider over the Internet. The services include providing

storage space or infrastructure over the Internet. The services can be free of cost or based on pay-per-use. Examples of public cloud systems are Gmail, Skydrive providing storage space, Amazon Web Services (AWS) containing the Elastic Compute Cloud (EC2), the Simple Storage Service (S3) offering IaaS and the Google App Engine with PaaS.

- **Hybrid Cloud:** A hybrid cloud service is implemented by combining the services of different cloud computing systems say combining private, public cloud. A hybrid cloud is created to fulfil the specific demands of the organisations. Hybrid clouds are complex to manage because communication between two or more cloud is needed. For example, an organization may have a public cloud service, such as Amazon Simple Storage Service (Amazon S3) to store their data but continue to maintain in-house storage for operational customer data. Windows Azure and force.com provides hybrid cloud structure.

1.1.3 Essential Characteristics of Cloud Computing

Cloud services exhibit essential characteristics that demonstrate their relation and differences from traditional computing approaches. According to (Mell & Grance, 2011) there are five characteristics of the cloud which represents its services.

- **On-Demand Self-Service:** The cloud users can have automatic provision of computing resources, as they need without requiring interaction with the cloud service provider. The user can increase or decrease storage space requirement, software as according to his need directly with on-line control panel. The user is billed based on pay per use policy.
- **Broad Network Access:** Cloud services are provisioned over the network and can be accessed via multiple devices such as mobile phones, laptops, PDA, etc. Services are available over the network with these devices wherever they are located with a simple on-line access point.
- **Resource Pooling:** The cloud service provider's resources are pooled in a multi-tenant environment; resources are dynamically allocated to the tenants according to their demand. It is independent from the location where data is saved. The tenants don't know the exact location of the resources. The shared resources include storage, processing, memory, etc.

- **Rapid Elasticity:** Cloud services can be automatically scaled at any time and at any quantity depending upon the user's demand. Depending on the need, user can add or delete resources and services at his site.
- **Measured Service:** Users usage of the provider's services is automatically monitored and reported providing transparency for both the user and provider. Measured resources can be storage space, software used, bandwidth, and active user accounts. Resources are monitored and reported, providing transparency to the user as well as to the cloud service provider.

1.1.4 Pros to the Cloud Computing

Cloud computing provides great expediency both to end users and enterprises of different size. With cloud computing the users need not to develop and maintain the infrastructure. The load is reduced as creation and development of the infrastructure is done at the cloud service provider site. According to (Buyya, Broberg & Goscinski, 2010) (Velte et al., 2009) (Amarnath Jasti, 2010), the benefits of the cloud computing for the company's and user's prospective are as follows:

- **Cost Efficiency:** By using cloud computing, there is no need to purchase costly software or servers. Cloud functionality, organizations can reduce licensing cost along with the reduction of overhead charge of data storage, software updates, and management. Cloud computing delivers the services based on the policy how much the customer has used the services.
- **Backup and Recovery:** Cloud backup for the user's data assures data protection and recovery. Cloud itself is replicated as a backup of the data located at different servers. Cloud services with recovery/backup options make the cloud reliable and flexible.
- **Convenience and Continuous Availability:** Wherever the end user might be located, public clouds offer its services over the Internet. Cloud computing provides easy data retrieval and serves the needs of geographically spread users. At the same time, it provides easier data access, viewing and modifying of shared documents and files. Cloud service provider uses many servers to obtain maximum duplicity. If there is

system breakdown, data can be retrieved from alternative instance on other machines.

- **Increased Storage Capacity:** The cloud services provide a large storage space to the users. Users need not to upgrade their hardware to increase the space time to time and cloud servers can be easily updated with large the storage space, which in turn reduces the infrastructure cost.

1.1.5 Cons to the Cloud Computing

Cloud computing is the technology with enormous benefits to the IT world. However, it also comprises security issues and inefficiencies. According to (Buyya et al., 2010) cons to the cloud computing are:

- **Possible downtime without Internet Connection:** Cloud computing services are completely dependent on the Internet connection. When the Internet connection or the network is down, cloud services are down as well. If the connection runs slow, the services will also run slow.
- **Security Issues:** Security is the biggest concern with cloud computing. Cloud computing is Internet based computing and using cloud infrastructure, takes away private data and confidential information from the user. The data is no longer on the user's hand with the cloud computing. Users have to trust their cloud service provider to protect their data from unauthorized users.
- **Compatibility with Cloud service provider's Existing Peripheral and Devices:** The peripheral needed for the cloud infrastructure are specific to the cloud service providers which lead to extra hardware cost.

1.1.6 Companies delivering services from the Cloud

The leading companies are looking forward to cloud-computing platforms to deliver services over the Internet to the users. There are various leading companies delivering services from cloud are as (Mather, Kumaraswamy & Latif, 2009):

- **Google:** Google delivers different kinds of services to its customers, which include email access, text translations, Google maps, web analytics etc. Google provides complete infrastructure to the users by launching its own

IaaS service, the Compute Engine. Google App Engine is popular Google's PaaS. Google also offers Cloud Storage space to the users.

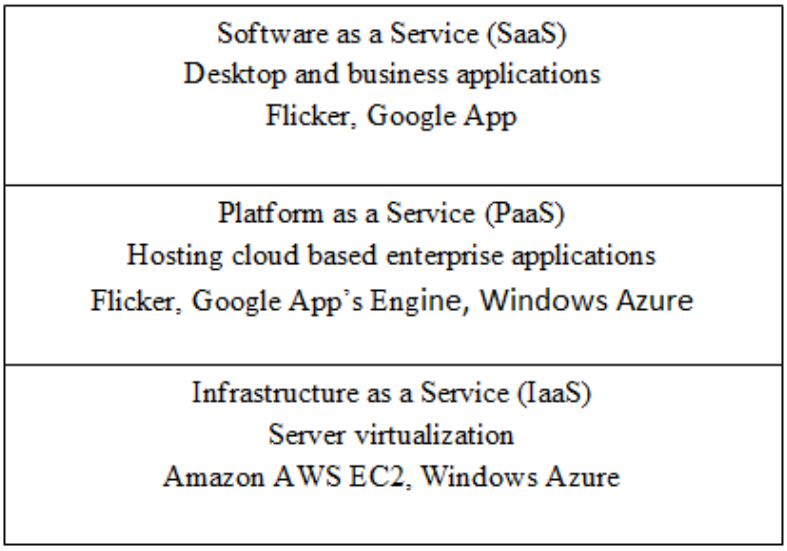

Figure1.2 : Cloud Delivery Model

- **Microsoft:** The Windows Azure platform of Microsoft offers PaaS of operating system and a fully relational database. Microsoft On-line Services are subscription-based, on-demand applications and hosted services, providing end users with a consistent experience across multiple devices including Microsoft Exchange On-line, Microsoft Share Point On-line and Microsoft Office Live Meeting.
- **Salesforce.com:** Salesforce runs its application sets for its users in a cloud. Force.com and Vmforce.com products provide platforms to the developers to build customized cloud services.
- **Amazon Elastic Cloud Computing (EC2):** Amazon EC2 is a component of Amazon's Web Services (AWS). It allows users to run computing applications in the Amazon EC2 data center. Amazon EC2 uses the Xen virtualization technique to manage physical servers.

1.2 Multi Tenancy – An Architecture of Cloud Computing

Multi-tenancy is an architecture in which a single instance of an application serves multiple users. Multi-tenancy is an important aspect of cloud computing to share resources among multiple users. Multi-tenancy allows multiple tenants to coexist in the same physical machine sharing its resources such as CPU, memory, network at the same time.

Cloud service providers make use of multi-tenancy to provide computing services to multiple customers by using a common infrastructure. In a multi-tenant environment, tenants have their own private space to save private data as well as global space shared among all tenants. By sharing resources and creating standard offerings, multi-tenancy offers reduced cost and optimum use of resources in a shared environment (Kalagiakos & Bora, 2012) (Jasti, Shah, Nagaraj & Pendse, 2010).

According to (Hao, Lakshman, Mukherjee & Song, 2010) sharing of resources between multiple tenants is fundamental to cloud computing. In IaaS, multiple tenants share infrastructure resources such as hardware, servers and data-storage devices. With SaaS, tenants are having the instances of the same application; data of multiple tenants is stored on the same database and may even share the same tables. The data of each must be isolated and remains invisible to other tenants.

Resources shared among multiple–tenants can be:

- Basic storage space
- CPU processing
- Memory
- Network bandwidth

Tenants are unaware of the other tenants with whom they share the resources by virtualization even they don't know the presence of other users sharing the infrastructure and the resources. This gives the tenants a sensation of privacy and personalization. As the co-existence of multiple tenants is unaware of each other, increases the security risks in cloud computing. It is important for the cloud service providers to ensure the security and isolation of the resources in the multi-tenant environment.

1.3 Virtualization

Multi-tenancy is obtained by using virtualization. It allows multiple operating systems to run on a single machine simultaneously. In cloud computing virtualization used to serve several end users by creating virtual version of storage space, operating system and hardware platform (Wu, Ding, Winer & Yao, 2010).

Virtualization divides a physical computer to several virtual machines known as guest machines. Multiple virtual machines run on a single host computer, each having its own OS and applications. Virtualization gives an illusion to the users that they are running their processes on a physical computer independently, but in reality, they are sharing the resources of a single host machine.

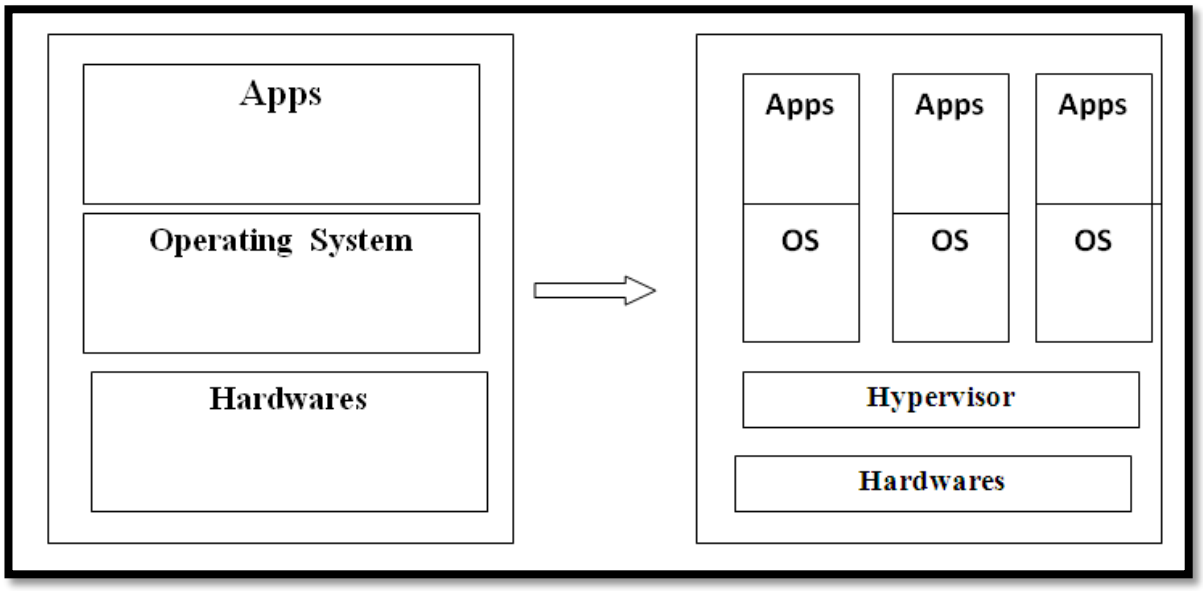

Figure1.3 : Independent OS to Virtualization of OSs

The figure1.3 shows how an individual operating system running its applications on the independent physical hardware can be placed in a virtual machine and share the same physical system with other virtual machines. It allows multiple operating systems (VM) to run concurrently on a single machine sharing its resources. Virtualization provides independence to the Guest virtual machines and efficiently distribution of hardware resources.

Virtualization gives an illusion to the processes on these virtual machines as if they are running on a physical computer independently, but in reality, they are sharing the physical hardware of the host machine. The software that allows multiple operating systems to use the hardware of the physical machine is called a hypervisor. Hypervisors sit between the operating system of the host machine and the virtual environment. As the tenant sharing the same physical host with unknowns, there are various kinds of risks associated with the multi-tenancy environment in the cloud computing. So it is an important aspect to isolate the multiple users on the same physical machine (Hwang, Zeng & Wood, 2013) (Sabahi, 2011).

1.3.1 Benefits of Virtualization

Different core technologies can be used to build cloud computing depending upon the organization needs. One of the most important and heavily relied technology in cloud computing is virtualization.

Some of the main benefits of virtualization are (Hwang, Zeng, Wu & Wood, 2013)**.**

- Reduce capital costs by increasing energy efficiency and requiring less hardware.
- Provision new servers when needed without the need to buy additional hardware.
- Hardware independence gives the freedom to move a virtual machine from one type of computer to another without making any changes to the device drivers, operating system or applications.

1.3.2 Types of Virtualization

According to (Jamsa, 2011) (Kalagiakos et al., 2012), there are four common approaches of virtualization with differences between how each controls the virtual machines.

- **Emulation virtualization:** A virtual machine simulates the entire hardware set needed to run unmodified guests for completely different hardware architectures.

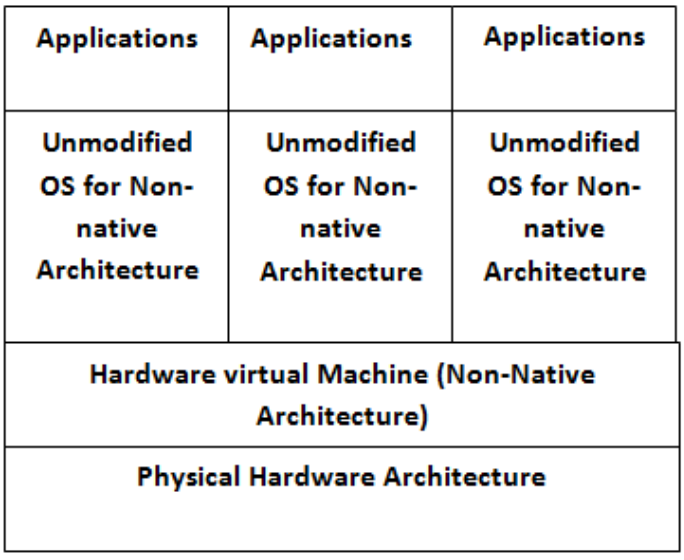

Figure1.4: Emulation Virtualization

Emulation virtualization used to create new operating systems for the hardware which is in design phase and not in the physical form. Bochs and QEMU provide emulation virtualization.

- **Para Virtualization:** Para means “beside” or “alongside”. Para virtualization is a server virtualization technique in which the guest operating systems are aware of being executed in a virtual environment. Hypervisor runs just above the physical hardware (Ring 0) so that guest OSs run in higher levels.

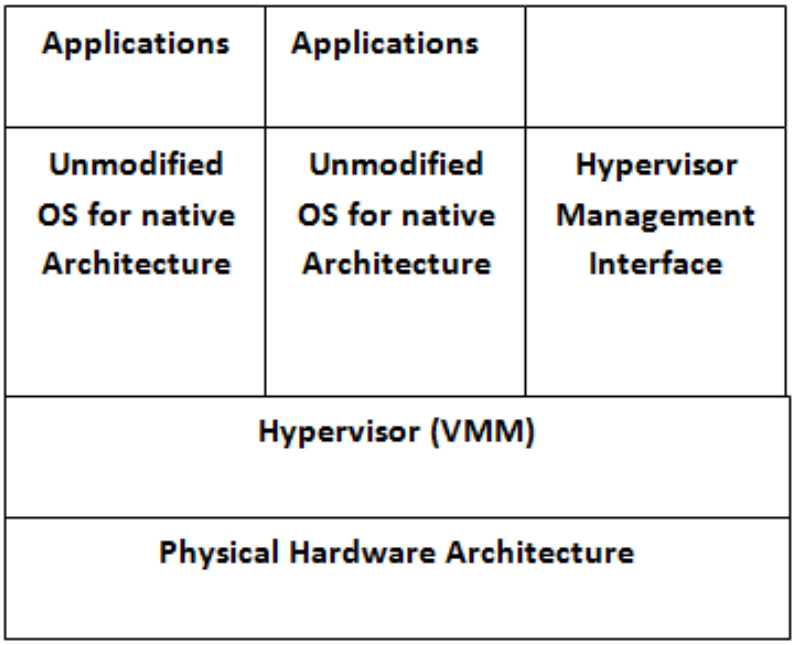

Figure1.5: Para Virtualization

It involves the modification of the operating system kernel to replace non virtualized instructions with “hyper calls” that communicate directly with the hypervisor. It involves low virtualization overhead. Xen and Hyper-V support Para virtualization.

- **Full Virtualization:** Full Virtualization is used to abstract the physical hardware resources to make a complete virtual system where the guest OS could be executed. Here guest operating systems are not aware of being executed in the virtualized environment. The Full virtualization is the highest level of virtualization that delivers services to the guest operating system with a virtual management layer (VMM).

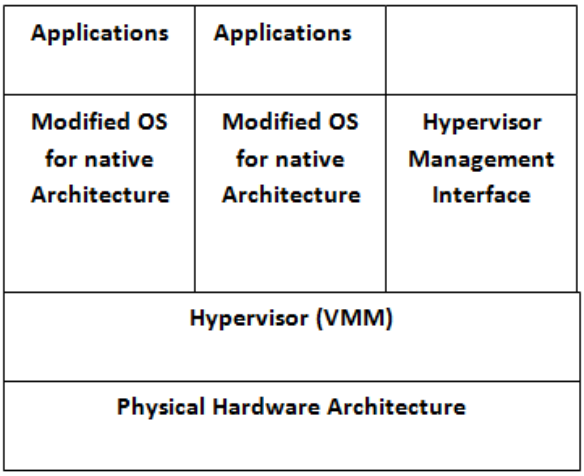

Figure1.6: Full Virtualization

With the ease of virtualization, the applications and software could be easily streamlined between different virtual machines. VMware ESXi, Microsoft Virtual Server supports full virtualization.

- **OS level Virtualization:** There is no requirement of virtual machine monitor software in OS level virtualization. Single OS handles all the guest images in different isolated containers.

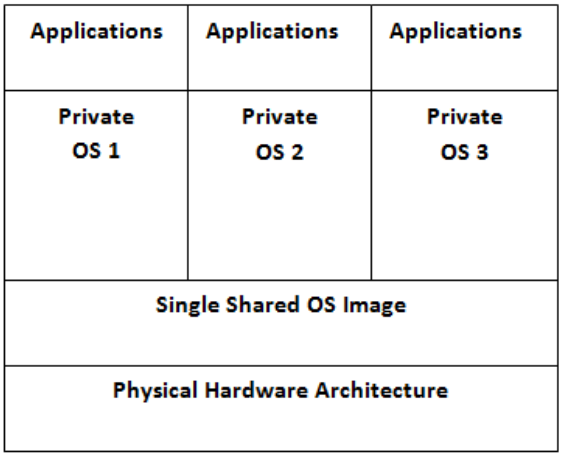

Figure1.7: OS Virtualization

OS level virtualization does not support running different operating systems (different kernel) at a time. Virtuozzo, Linux VServers and OpenVZ provide OS level virtualization.

1.4 Hypervisor

The hypervisor is a software layer which manages the virtualization, allows multiple Guest operating systems (VMs) to run concurrently on a single machine.

Hypervisor provides independence to the Guest virtual machines and efficiently distribution of hardware resources. There are numerous hypervisors ranging from open-source such as KVM, Xen and virtual-box, to commercial hypervisors such as VMware ESXi and Microsoft Hyper-V (Brunette & Mogull, 2009).

1.4.1 Types of the Hypervisor

The hypervisor is directly responsible for hosting and managing VMs running on the host. It provides a virtual hardware that is comprised of a configuration file, some virtual disk files and various other files such as non-volatile RAM. Type 1 and Type 2 hypervisors differentiate whether the host operating system is present or not.

- **Type 1 Hypervisor:** A Type 1 hypervisor also known as “Bare metal” is a piece of software or firmware that runs directly on the hardware.

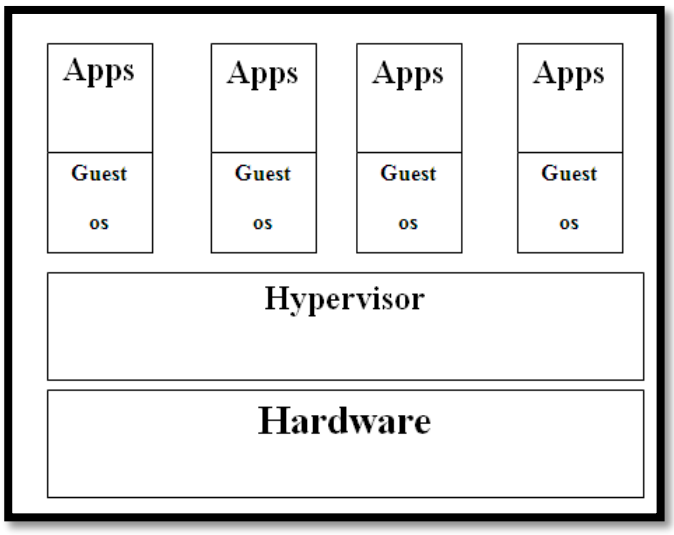

Figure 1.8: Type 1 Hypervisor model

It is responsible for coordinating access to hardware resources as well as hosting and managing VMs. It is completely independent of the operating system. VMWare ESXi, Xen are Type 1 hypervisors (Jasti et al., 2010).

- **Type 2 Hypervisor**: A Type 2 hypervisor also known as “hosted” runs as an application on an existing operating system. Type-2 hypervisor sits on top of an operating system. This type of hypervisor emulates the physical resources required by each VM. Type-2 hypervisor relies heavily on the operating system.

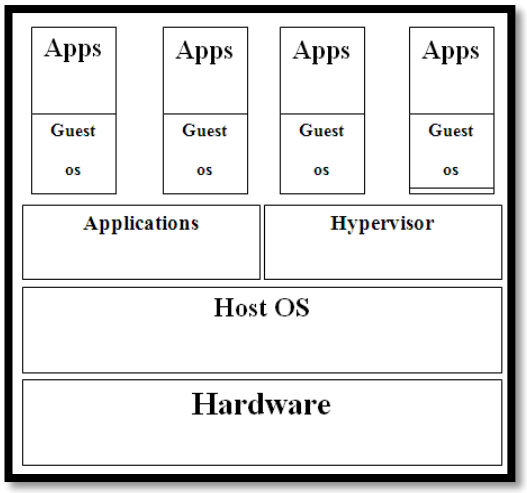

Figure 1.9: Type 2 Hypervisor Model

It cannot boot until the operating system is already up and running, if for any reason the operating system crashes, all end-users are affected. VMware Workstation, Virtual Box and KVM are examples of Type 2 hypervisors (Jasti et al., 2010).

1.5 Security in Multi-Tenant Environment

As the tenant sharing the same physical host with unknowns, there are various kinds of risks associated with the multi-tenancy environment in the cloud computing. So it is an important aspect to isolate the multiple users on same physical.

It is very difficult to secure the VMs because of the upcoming techniques on how-to-attack a VM or gain control over the Hypervisor. VMs are mobile so they could be easily located on different hypervisors as per the availability of the resources. The security policies for such a mobile VMs should be very secure, which needs to be assured with the other hypervisor's security policy. If the security policy doesn't accompany, then the VM becomes vulnerable (Dawoud, Takouna & Meinel, 2010).

So there is a need to enhance the isolation in the virtualized cloud to provide security and ensure the cloud is secure and safe. The cloud service provider must take the preventive measures against the security issues.

The VM threats, attacks or vulnerabilities can pose a great impact on the OS. An attacker if able to gain access over the Hypervisor, then the whole server

could be at risk. All the VMs running over the hypervisor would be compromised (Reuben, 2007).

1.5.1 VM-to-Hypervisor Attacks

According to (Hwang, 2013) (Jasti et al., 2010), hypervisor is the main source of managing a virtualized cloud platform; the attackers target it to access the VMs and the physical hardware.

As the hypervisor resides between VMs and hardware, the attack on the hypervisor can damage the VMs and hardware. Security VMs is compromised due to some attacking vulnerabilities at the hypervisor.

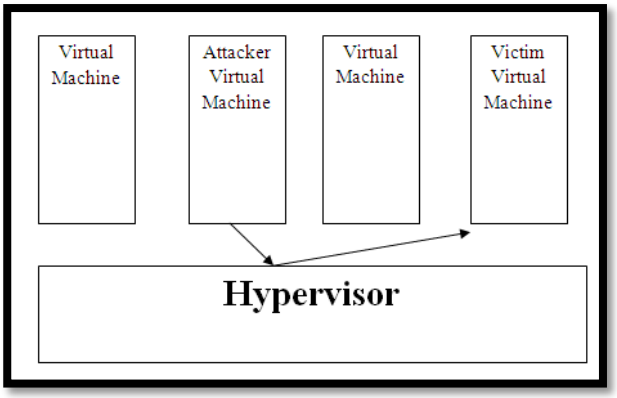

Figure 1.10: VM to Hypervisor attack in Virtualization

An attacker tries to escape from the isolation created by the hypervisor, can potentially access the host OS and the other VM. The attacks over the hypervisor to access the host or the guest VMs are VM Hopping, VM Escape and Mobility.

- **VM hopping:** VM hopping is the process of hopping from one VM to another VM. An attacker being on one VM can gain access over the other VM. This can be achieved if both the VMs are running on the same host. An attacker on VM can gain access over the other VM on the same host by just knowing the IP address of the other VM or gaining access over the host itself. Once a VM is attacked, the attacker can monitor the traffic going over the VM and change the flow of traffic or manipulate it. This attack can create issue of Denial of Service (DoS) which is actually an attempt to make a computer resource unavailable to its intended users; also the attacker can change the files of the VM by changing the configuration file. If VM is running since a long time, an attacker can modify the configuration file such

that the victim VM goes to off state. Therefore, the ongoing communication could be stopped. Also it can abruptly stop, so the communication is incomplete. When the connection is resumed, the VM needs to restart the entire communication.

- **VM Escape:** VM escape is a vulnerability in the virtualization that enables a guest-level VM to attack on its host OS. An attacker runs a code on a VM that allows the break out of the virtual machine and interacts directly with the hypervisor. VM Escape means gaining access over the Hypervisor layer and attacking the rest of the other VMs. If an attacker able to gain access to the host running multiple VMs, the attacker can access the resources which are shared by the other VMs. An attacker can bring down these resources and turn off the hypervisor. If the hypervisor fails, all the other VMs turn off eventually.

1.5.2 VM-to-VM Attacks

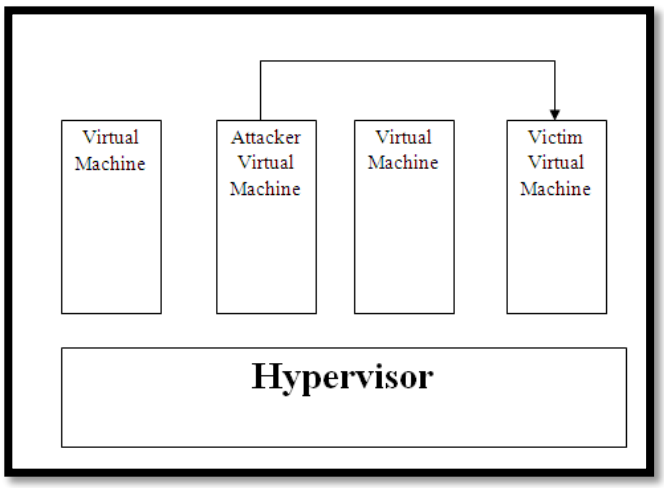

Figure 1.11: VM to VM Attack in virtualization

The co-existence of multiple VMs on a single piece of hardware presents malicious VM owners with the opportunity to glean potentially sensitive information from victim VMs sharing the same hardware resources (Wu, Ding, Winer & Yao, 2010).

An attacker may use guest OS (Virtual Machine) try to communicate and compromise other Virtual Machines on the same physical host therefore, breaking the isolation characteristic of VMs. The most common attacks under this are

Measure cache usage, Sniffing attack and Spoofing attack that lead to Denial of Service (DoS) attack.

- **Sniffing Attack:** All the Virtual machines share a common network on a host machine. There is a possibility of traffic sniffing when the VMs communicate with each other. The hypervisors offer virtual network to link VMs using virtual bridge and route. In virtualized environments, virtual Hubs are created to share the same network in the bride mode. If these hubs are not properly configured, the malicious attackers can try to sniff traffic to its own VM that is directed to other VM on the network. The malicious VM can use sniffing tools like “wireshark” to sniff the virtual network traffic. By using these tools an attacker can sniff IP address of the other VM that is an available neighbor to it. The attacker can perform packet sniffing attack over the victim. As a result, isolation is easy to be broken (Hwang, Zeng & Wood, 2013).
- **Spoofing Attack:** In the route mode, virtual switches are used to connect the virtual machines to the host machine. The virtual switches need a dedicated interface to connect each VM. Media access control (MAC) address is assigned to each virtual machine. As the address resolution protocol (ARP) is necessary to implement to redirect VMs’ traffic over the network. The routing table is maintained by sending an ARP command to each VM in boot time. A common vulnerability of ARP is ARP spoofing attack because ARP does not require proof-of origin. It is possible for the attacker to claim any MAC address by issuing the ARP reply message with his IP. Hence the attacker can use ARP spoofing attack to redirect all the traffic of a victim VM to his VM (Wu et al., 2010).

1.5.3 Denial of Service (DoS) Attack

A denial-of-service attack is defined as preventing a system to deliver services from its normal behaviour. DoS attacker tries to prevent the legitimate user to access the services from the server. To perform the denial of service attack, the attacker consumes all resources of that system, thus preventing other users gaining access to those resources results Denial of Service.

The attack attempted by multiple people in a Distributed environment lead to Denial of Service attack. The attacker does this by commanding remotely controlled computers to flow network traffic at the victim. The victim becomes so busy with dealing request from these systems and not able to respond legitimate users' requests. The systems that are involved as attacking agent known as Zombie and a large group of zombie computers is called a robot network, or botnet.

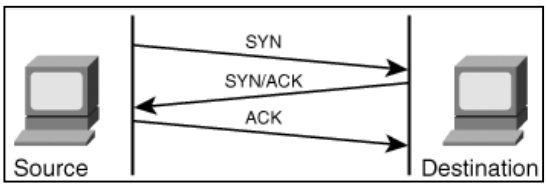

Figure 1.12: TCP Three Way Handshake

TCP/IP is a connection oriented networking protocol that starts with "handshaking" in client-server architecture. TCP provides reliable delivery of data. To establish a connection the client, firstly, sends a "SYN" packet to the server.

Then the server replies with a "SYN/ACK" packet that signals the server is ready to accept the connection. Finally, the client sends an "ACK" packet to establish the connection. As the connection established in three steps, the procedure known as "Three-Way Handshaking".

TCP connection is exploited to perform DoS attacks by TCP SYN flood. The attacker takes advantage of the three-way handshake in order to exhaust the resources. An attacker tries to overload the victim with so many TCP connections request that it will not be able to respond to legitimate requests. The attacker sends too many TCP SYN packets to the victim.

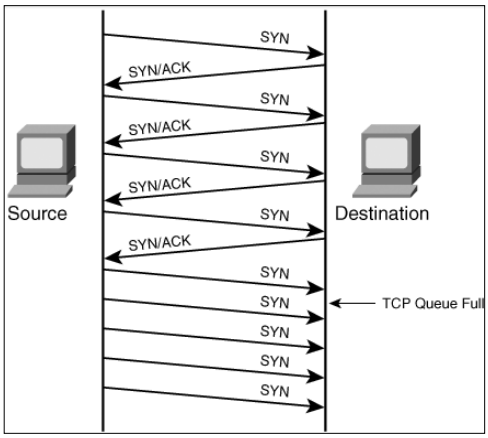

Figure 1.13: TCP SYN Flood

The victim allocates buffers for each new TCP connection and transmits a SYN-ACK in response to the connection request. The attacker does not respond to the SYN-ACK. In this way, large numbers of half-open connections are maintained on a victim server's queue, and it gets full. The queue of the server is limited, and legitimate client's request cannot be fulfil due to unavailability of the resources (space) in the queue (Kavisankar & Chellappan, 2011), (Schuba, Krsul, Kuhn, Spafford, Sundaram& Zamboni, 1997).

Dos attacker uses the IP spoofing to perform the attack. IP spoofing is the creation of IP packets with forged IP source addresses. Denial of service attacker uses the IP spoofing for hiding the identity of the sender. In DoS attack, the attacker floods the packets with the overwhelming amount of traffic and does not care about receiving back the IP packet's response. IP spoofing uses randomized IP addresses to start the three-way handshake. IP spoofing is difficult to filter as spoofed packets appear to be coming from a different address. The attacker uses subnet spoofing, spoofs a random address within the address space of the sub network (Kavisankar & Chellappan, 2011).

- **DoS attack in cloud computing:** In the virtualized environment all the virtual machines and the host machine are sharing common resources such as storage space, network bandwidth, CPU usage. The denial of service attack is aimed to exhaust the common resources from the host machine in order to deny the services to other guest virtual machines. In Denial of service attack, one machine receives more requests than its capacity and other end users requests cannot be served. In the cloud environment, DoS attack is more dangerous than unclouded environment because of VMs are sharing their resources with other virtual machines over the same physical machine. One virtual machine can perform denial of service attack to another virtual machine as well as to the host machine in the virtualized environment. The Transmission Control Protocol (TCP) provides reliable delivery of data over the Internet. TCP can be exploited to perform denial of service attack known as TCP SYN flood attack. As a TCP connection is established by three-way handshake, and the attacker takes advantage of this. An attacker overloads the victim with so many TCP connection requests that it will not be able to respond the legitimate requests. This is

done through sending too many TCP SYN packets to the victim virtual machine. The victim allocates buffers for each new TCP connection and transmits a SYN-ACK in response to the connection request. The attacker VM does not reply to the SYN-ACK packets (Bakshi & Yogesh, 2010) (Brohi, Bamiah, Brohi & Kamran, 2012) (Ryan & Liu, 2012).

Cloud computing can be provided by different levels such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS). The services provided can be deployed on different type of cloud such as public cloud, private cloud, community cloud and hybrid cloud. The development of virtualization has been an important factor in the development of cloud computing. However, virtualization doesn't provide complete isolation due to some potential attacks in it.

1.6 Problem Statement

The whole networking in the virtualization is done through the Hypervisor. The hypervisor allows inter VM communication by creating a network. Due to inappropriate security standards used for hypervisors at the infrastructure level, there are security gaps that can be exploited by the inside or outside malicious attackers to misuse the infrastructure.

The vulnerability of potential attacks from malicious virtual machine to its neighbor virtual machine in same physical infrastructures exploits the isolation in virtualized cloud computing. Denial of service (DoS) attack which aims to exhaust the resources, which kind of attack can effect on cloud performance in general and can cause financial Losses.

DDoS attack is more effective in the cloud environment because cloud users share the computing resources and data-storage space among themselves even with potential attackers who are connected through the same switch. The firewalls at the hypervisor level could not provide complete defense from DDoS attack to a guest virtual machine. The hypervisor firewalls mitigate the DDoS from outbound traffic of the network. But if the internal malicious VM attacks over another VM in the network by using subnet spoofing, the hypervisor level firewalls could not control the vulnerability.

There is a need of a mechanism at the VM level to secure the guest virtual machines from the internal network attacks.

1.7 Proposed Model

TCP SYN Flood exploits the underlying structure of TCP/IP three-way handshake. A well configured firewall at the hypervisor can't fully stop the DDOS attack from the internal network. The proposed scheme is concerned with the detection and mitigation of TCP DDoS attack – it will include:

- Deployment of private virtualized cloud with a malicious VM.
- The firewalls at the hypervisor level and at the VM levels are to be implemented to prevent from internal network attack.

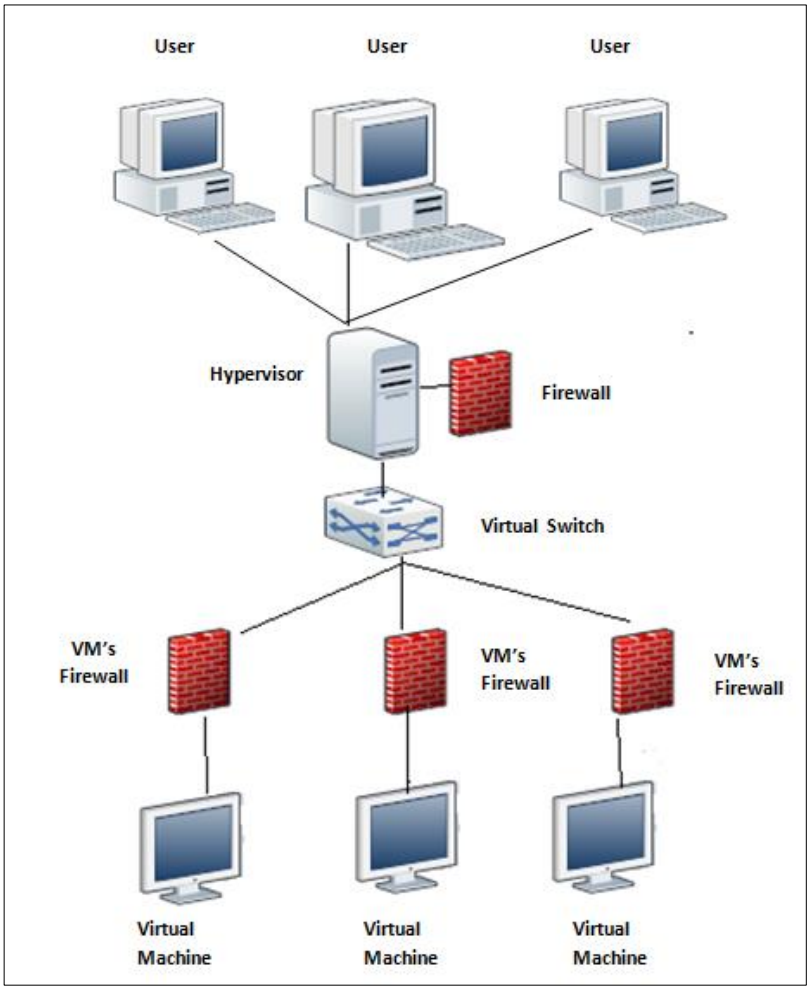

Figure1.14: Proposed model of VMs with firewalls

- The admin configures the firewall at each virtual machine in the network. The traffic is to be intercepted by the VM before it reaches to it and TCP/IP packets are filtered, shaped and limited once a threshold has been reached.

1.8 Objectives of Dissertation

The objectives of the research are:

- To detect the DDoS attack on the virtual machine by the internal VM on the same physical host.
- To mitigate the effect of DDoS from Virtualization.
- To enhance the isolation from DDoS attack between various VMs on the single host.

1.9 Scope

The dissertation mainly focuses on the Cloud computing and virtualization issues related to the cloud computing. Cloud computing is the leading technology in the IT world; the organizations are moving to the cloud due to its financial benefits and flexibility. However, the cloud service providers don't ensure the data security completely that limits the organizations to move to the cloud. Researching in virtualized cloud computing would help remove some of the obstacles in the technology and pave a way for future research. This dissertation aims to explore various attack vectors in the multi-tenancy and virtualization in a private IaaS cloud. The research focuses on the threats arisen from malicious tenants to the co-existing tenants in the same physical host.

The different security issues will be also explored in order to provide an introduction to the main focus of the research. A critical analysis of the DDoS will be provided along with the mechanism on how to approach it. The research approaches to the robust security model to improve cloud computing technology in the IT world.

1.10 Dissertation Outline

The dissertation is organized in five chapters following this introductory chapter, chapter 2 presents a literature survey of books, articles, published papers. It provides an overview of cloud computing, virtualization as well as review of the security concerns related to the current cloud computing model.Chapter3 involves the research methodology used; it explores how a malicious VM can attack over VMs present in the network. The different steps to run successfully an attack is described and analyzed. Chapter 4 includes the results that show the

detection of DDoS attack over the victim VM and mitigation by the firewalls at the victim site. The dissertation concludes with a set of protocol implementation recommendations and further research suggestions in chapter 5.

The chapter describes the Cloud computing as an Internet based computing with pool of shared resources. Cloud computing makes use of multi tenancy and virtualization that bring security issues to the technology. A review of VM to VM attacks and VM to hypervisor attack led to the formation of research question “Vulnerability of DDoS attack by a malicious VM can exploit the TCP Three Way Handshake at the victim VM in the virtualized cloud network”. A model is proposed to detect and mitigate the TCP–DDoS at the victim VM site.

CHAPTER-2

REVIEW OF LITERATURE

2.1Background

Several books **Velte et al. (2009)**, **Mather et al. (2009)** and papers **Reuben (2007)** have covered the concept of cloud computing. Cloud computing is the leading technology in IT and business world, thus there are multiple definitions.

Mell & Grence (2011) the National Institute of Standards and Technology presents a well-recognized description for cloud computing, including its characteristics, service models and deployment models. NIST defined that the security of full virtualized cloud is completely dependent on security of each of its components i.e. the hypervisor, host OS, guest VMs, applications and storage. Organizations should secure all of these elements.

The books **Buyya et al. (2010), Rhoton (2009)** covers the definitions, benefits, security issues, services and all the other areas and aspects related to cloud computing.

Cloud Security Alliance **Brunette & Mogull (2009)** presents the cloud as a collection of services, applications, infrastructure comprising a pool of network, information, and storage resources. The document for security guidance provides an overview of cloud computing, supporting NIST's definition. It includes 12 areas of security concerns associated with the cloud computing and recommendations for each one.

2.2 Literature Survey

One of the significant challenges in the cloud computing is security issues in the technology. Bamiah & Brohi (2011), Turnbull & Shropshire (2013) explores the various kinds of attacks and vulnerabilities of virtualized cloud computing, along with the threats arisen from malicious virtual machine to co-existing virtual machines.

Reuben (2007) presents different kinds virtualization technologies in the cloud computing along with the various challenges concerning security in virtual machine environment. Majority of the security issues presented are concerned

with the security of the host machine and the hypervisor software layer. If the host or the hypervisor is compromised by the malicious VM then the whole security of the system is broken.

Dawoud et al. (2010) presents the infrastructure as a service component's security vulnerabilities and privacy concerns. Cloud software's security that impacts the IaaS is considered. Potential threats to the hypervisor are depicted by the authors. Trusted virtual Data centre technique is proposed to improve the confidentiality of data and integrate the scheme to manage the resources at the hypervisor level.

Jasti et al. (2010) presents the virtualized cloud computing services where the physical resources are transparently shared by between the multiple VMs that co-exist on the same physical machine. Security threats that are associated with a virtualized cloud computing environment are explored. It explores the threat that a malicious user having control of a virtual machine can try to gain control over other VM's resources or utilize all system resources that may lead to denial of service attack over other VM users. The malicious VM user can also steal the data of other VMs located on the same physical machine by compromising hypervisor file system. It explores how isolation of such co-existing VMs can be exploited to gain access over other user's VM.

Szefer & Lee (2011) presents the hypervisor as the comprehensive part of virtualization technology. A hypervisor is a software management layer that can access all resources of the infrastructure. The attackers monitors the guest VMS by compromising the hypervisor. The authors proposed a technique to tackle the threats that compromise the hypervisor. The work focuses on hardening hypervisors to make it more secure. It added up new hardware mechanism in the multicore microprocessors to protect the guest VMs from the compromised or attacked hypervisor, but the technique includes much limitation; it didn't consider the DDoS attack in the virtualization along with the assumption no malicious modification is done to the hardware.

Sabahi (2012) proposed the virtualization architecture by converting the centralized security system to a distributed one. The distributed security system reduced the workload from hypervisor-based virtualization, but the distribution

security system is complex to handle as the infrastructure expands. The scheme may inject new vulnerabilities to virtualized cloud computing.

Kalagiakos & Bora (2012) proposed a technique which aims to enhance security and revolve directly or indirectly around the hypervisor. The mechanism provides security from VM to hypervisor attacks only, it doesn't consider the cross channel i.e. VM to VM attacks.

Subashini & Kavitha (2013) presentsan analysis to the various unresolved security threats in virtualized cloud computing, which are affecting infrastructure as a service. The author described the pros and cons to the existing security techniques. Due to the complexity of cloud architecture, it is very difficult to achieve security. New security techniques need to be developed, and older security techniques needed to be twisted to work with cloud infrastructure.

2.2.1 DDoS Attack in Cloud Computing

Denial of Service attack aims to exhaust the resources at the victim site. A denial-of-service attack is aimed to prevent a system to deliver services from its normal behaviour.

Zuquete (2002) presents TCP SYN cookies as protection against TCP SYN Flood attack. It prevents the denial-of-service scenario by not keeping state about pending connection requests, or half-open connections. The cookies allow a server host to maintain the state of half-open connections outside its memory such state is (partially) stored inside a cryptographic challenge, the SYN cookie is returned to the client within SYN-ACK segments as the server's TCP Initial Sequence Number (ISN). Since TCP requires the client to send back that ISN on the subsequent. ACK, the server will be able to restore a half-open connection from a cookie and, consequently, create a final connection descriptor.

Wang, Zhang & Shin (2004) presentsTCP SYN Flood as the type of denial of service attack.SYN floods are detected by monitoring statistical changes in numbers of SYN and FIN packets. Under normal conditions, numbers of SYN and FIN or RST packets are equal. However, during the attack, the victim is unable to respond to a majority of SYN packets so the ratio is changing. But the generic algorithm cannot identify the attacker in the virtual environment and even cannot detect the attack; because in a virtualized environment, there is a wide variety of

network topologies and the host cannot distinguish the ownership of the packets, which is different from physical network.

Eddy (2006) presentsTCP SYN Flooding attack that exploits the structure of Transmission Control Protocol (TCP), to make the victim incapable of answering a legitimate user's requests for new TCP connections. There is no single protection strategy for TCP implementations. It described the attack and network simulation to prevent SYN flooding attacks.

Mirzaie, Elyato & Sarram (2010) presents a model that prevents the DDOS attack by limiting on the number of connection and the packet delivered in time. Iptables has the number of packets sent through a connection. The Iptables firewall rules limit the number of SYN packets that a specific user can send a specific number of SYN packets within certain intervals. The server also set the limit for the total number of connection at any moment. The firewall rules can prevent SYN Flooding attack from a specific user but in case of IP spoofing, the firewalls could not prevent the attack.

Wu et al. (2010) presents the networking security issues in the virtualized cloud computing. The author outlines the security issues in virtual machines that are raised due to inter VM communication. It discusses the various kinds of networking attack, i.e. ARP poisoning, IP spoofing that lead to denial of service attack over the virtual machines.

Bakshi & Yogesh (2010) proposed architecture to employ intrusion-detection sensor SNORT on the virtual interface which sniffs all the traffic in-bound and out-bound over the Internet. But the IDS could not prevent the DDOS attack if the malicious user existing in the same network and perform the SYN flood via subnet spoofing.

Nazri, Aborujilah, Musa & Shahzad (2012) presents denial of service attack as the most harmful attack in the virtualized cloud environment than unclouded environment because in the cloud computing environment, the VMs are sharing their resources and confidential data to the unknown co-existing VM and even don’t know their presence. One virtual machine can be the source of denial of service attack to another virtual machine existing in the same infrastructure.

Wei, Xiaolin, Wei & Si (2012) proposed a model that detects DDoS attack on the basis of the change of input flow and output flow number of SYN and RST+FIN packets, but the method is based upon the feedback algorithm that detects the attack after the attack has been implemented.

Shea& Liu (2013) presents the performance degradation of the VMs in the virtualized cloud environment due to denial of service attack. Experiments are evaluated to examine the performance of virtualized cloud under the denial of-service (DoS) attack. It explores the results that on a the denial of-service (DoS) attack, the performance of a web server in a virtualized cloud degrades up to 23%, while that of a non-virtualized degrades by only 8%.

Brunette & Mogull (2009), Bamiah & Brohi (2011), Dawoud et al. (2010) presents cloud computing as a new IT model with several benefits. However, there are many security concerns that must be dealt with first. As multi-tenancy, virtualization comes with its own issues. The hypervisor provides a new attack surface to be compromised, and the virtual network enables a malicious VM to perform attacks on other. These attacks lead to the denial of service attack that can exhaust resources of the co-existing VMs.

CHAPTER- 3
RESEARCH METHODOLOGY

The chapter represents an implementation of the research work as described in the previous chapters. The work is divided into two main parts. The first part includes the private cloud infrastructure deployment through the installation of a hosted hypervisor VMware ESXi and the interface vSphere client to access the virtual machines. The second part describes the implementation of the attack over the virtual machine via a malicious virtual machine existing in the same network.

3.1 Environment Setup

To deploy the private cloud infrastructure, the physical server VMware ESXi Hosted Hypervisor is installed that provides sharing of different resources such as CPU, memory, Network Interface Card (NIC) to multiple VMs in the host only mode. The vSphere Client is the interface that accesses and manages the multiple VMs remotely.

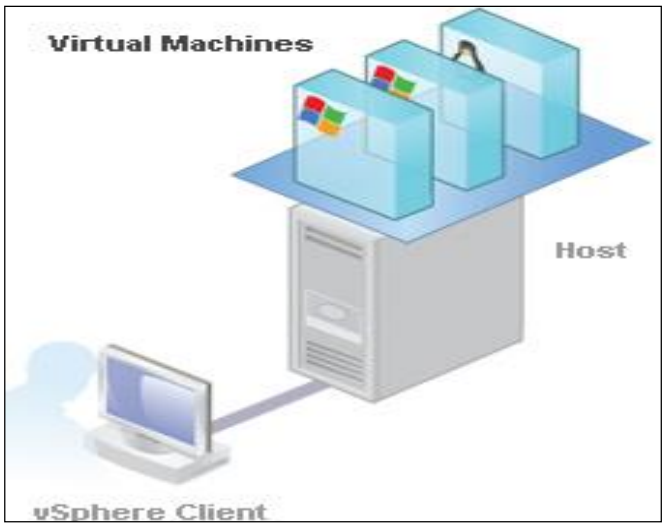

Figure 3.1: Virtualized cloud infrastructure

The cloud component includes VMware hypervisor, vSphere client and the virtual machines.

3.1.1 VMware ESXi (The hypervisor)

VMware ESXi is a type 1 Hypervisor that supports the full virtualization. ESXi shares the processor, storage, memory and resources into multiple VMs.

Figure 3.2: ESXi DUCI

In ESXi, the resources are shared amongmultiple VMs according to each user's need. ESXi uses the DCUI (Direct Console User Interface). DUCI is a simple menu-driven interface for setting up administration access, configurations and troubleshooting.

3.1.2 The Management Client (vSphere client)

The vSphere Client is the interface for ESXi data store management and to access VMs. vSphere client provides the access to the VMs and manages the ESXi server remotely.

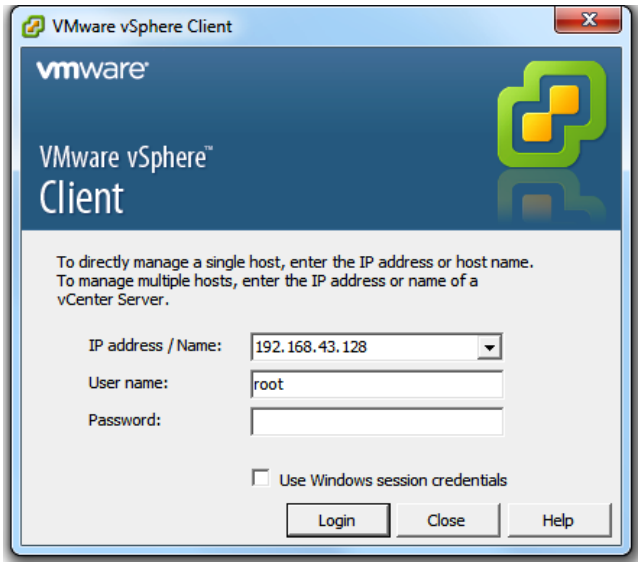

Figure 3.3: vSphere Client connection window

The vSphere client provides information about the host, processor, memory,hard drives and networks as well as the number of physical NICs and virtual machines. It also shows the current CPU and memory utilization.

3.1.3 Virtual Machines

The VMs are accessed through the vSphere client. Under the single host VMware ESXi hypervisor several VMs are operated with different Operating systems via vSphere client. Each virtual machine contains individual IP addresses, which can be pinged and accessed from a remote location by the different users just like stand-alone hosts.

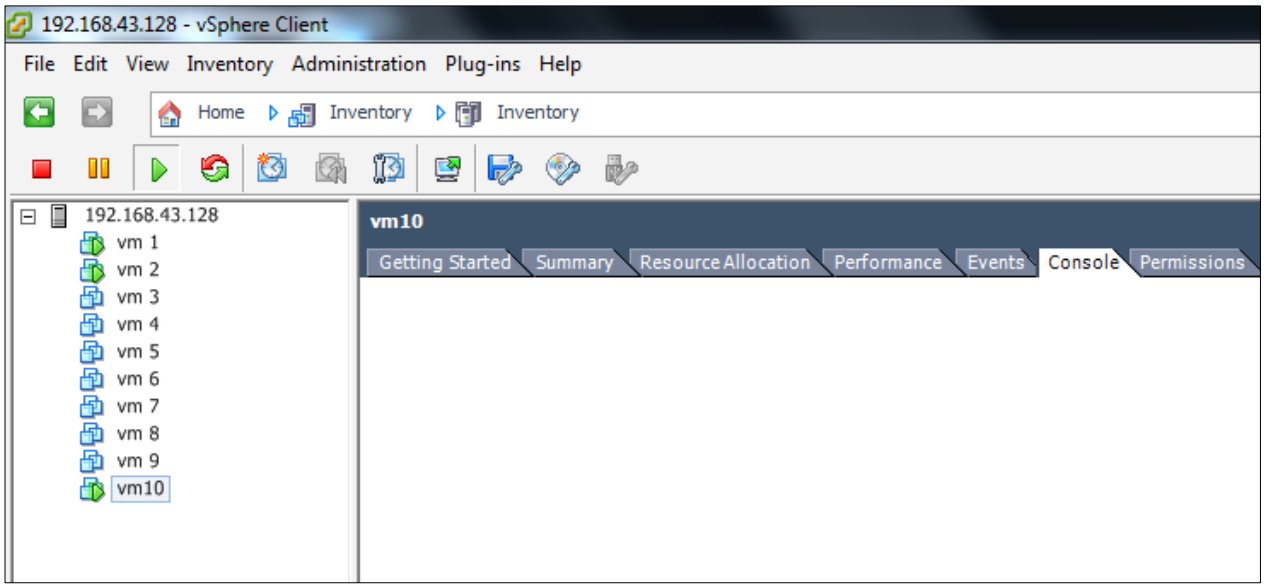

Figure 3.4: vSphere Client with VMs

Virtual machines have the same functionality as the physical hardware they are hosted in. A VM is backed by the physical resources of the host. Configuration of the installed virtual machines to conduct the research is as follows:

The Victim VM

- Virtual Machine Name: vm 1
- Guest operating system: Ubuntu 14.04 lts
- Number of virtual CPUs: 1
- Amount of RAM: 2048 MB
- Physical-Memory: 8 GB
- Number of vNICs: 1

The Attacker Virtual Machine

- Virtual Machine Name: vm 10
- Guest operating system: Backtrack 5r3
- Number of virtual CPUs: 1
- Amount of RAM: 256 MB
- Physical-Memory: 1 GB
- Number of vNICs: 1

Other Virtual Machines

- Virtual Machine Name: vm 2 to vm 9
- Guest operating system: Backtrack 5r3
- Number of virtual CPUs: 1
- Amount of RAM: 256 MB
- Physical-Memory: 1 GB
- Number of vNICs: 1

3.2 Performing Attack

To conduct the research, ten guest virtual machines are installed over the hypervisor and accessed through the vSphere client. Among the guest OS (VMs) one machine with the IP address 192.168.43.129 is the malicious node and sniffs the network traffic to know about the other tenants present in the network. The attacker VM acts as a source of the TCP SYN flood packets to another VM existing in the same network. The victim VM with the IP address 192.168.43.138 receives TCP SYN packets more than its capacity, and its resources get exhausted. The other virtual machines are used as Zombie that is connected on the same network segment as the host and guest virtual machines.

3.2.1 Network Scanning

Using the ‘nmap’ tool the attacker virtual machine performs the scan to know about the other virtual machines IP addresses present in the network.

The ‘nmap’ reports co-existing VM’s IP addresses along with status, whether the VM is online or offline. The VMs with green symbol are currently online, and the VMs with red symbol are currently offline in the network.

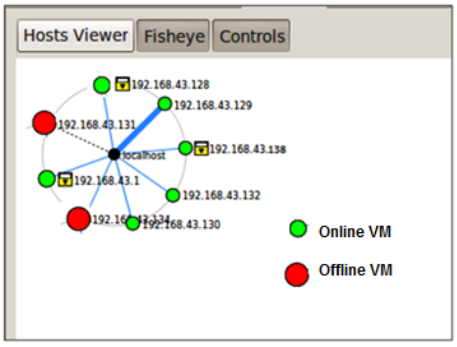

Figure 3.5: Nmap scanning result

Now the attacker VM picks the online co-existing VM with IP address 192.168.43.138 to perform TCP-SYN flood.

The attacker VM scans the VM to check for the open TCP ports to perform the attack with the 'nmap'.

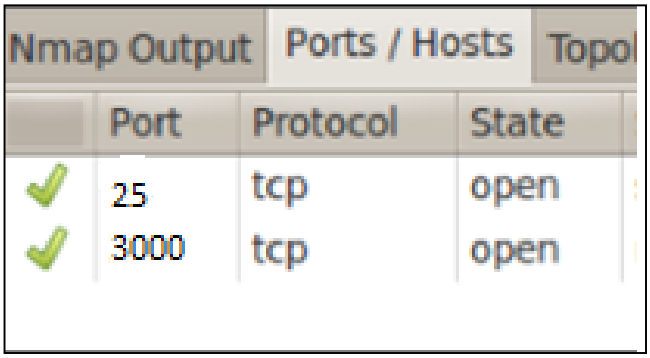

Figure 3.6: 'nmap' tool scanning for the open ports

The scan showed for the IP address '192.168.43.138' TCP port 25 and TCP port 3000 are open.

3.2.2 TCP-SYN Flood Attack

The attacker virtual machine makes use of hping3 tool to SYN flood the target in a distributed manner with the direct IP address, random IP spoofing and spoofed IP addresses of other virtual machines that are offline or online in the network. The virtual machine uses full capacity of its processor to flood the host with SYN requests.

3.2.2.1 Direct Attack

The attacker VM rapidly sends TCP SYN packets with its own IP address as the source. Hping tool is used to flood the victim VM with TCP SYN request.

The command used to flood TCP SYN request is:

sudo hping3 -flood -S -p 3000 192.168.43.138

The command floods the TCP SYN packets to the TCP- Port 3000 on 192.168.43.138.

-S: Specifies the SYN Flag

-p: Specifies the TCP Port

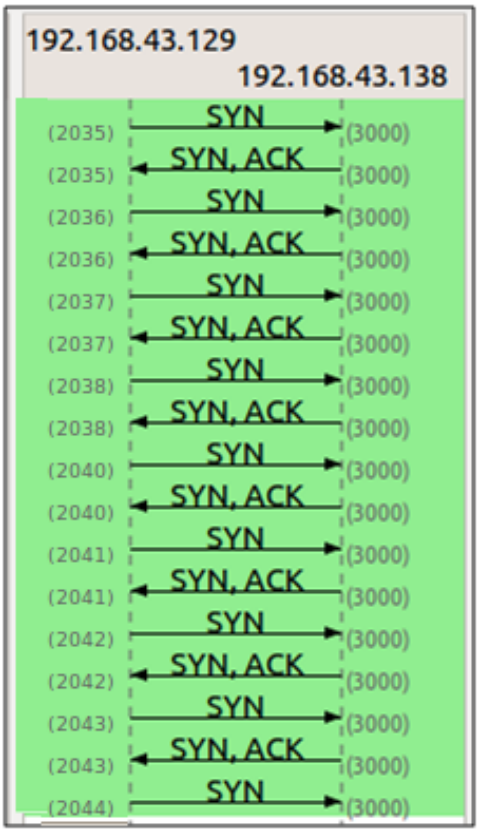

Figure 3.7: SYN Flood with own IP address

The scenario shows that the attacker VM initiates the TCP connection by sending SYN packets and the victim VM replies with the SYN-ACK packet, and then the attacker doesn't send the final acknowledgement to complete the three-way handshake. At the victim VM site, high numbers of half-opened connections are left. The queue that is storing the half opened connections is of finite size, and it is made to overflow by intentionally creating too many half-open connections. The victim keeps on waiting for the final ACK packet and after the RTT (round trip time) expires; it resends the SYN-ACK packets to the attacker. The victim VM is not able to further create new TCP sessions for the legitimate network traffic.

3.2.2.2 Random Spoofing Attack

The malicious virtual machine floods TCP SYN packets to the victim virtual machine with the random source address.

The command used to flood TCP SYN request is:

sudo hping3 -flood -S -p 3000 192.168.43.138 –-rand-source

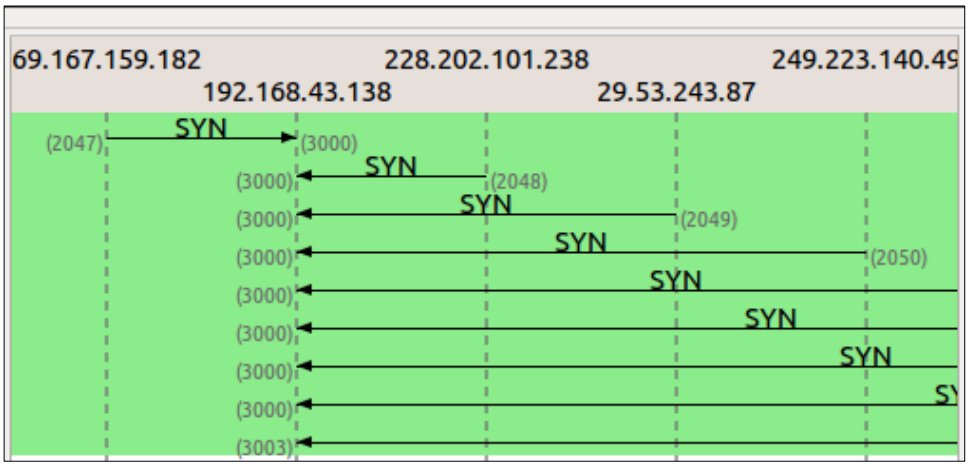

Figure 3.8: SYN Flood with random IP spoofing

The figure 3.8 shows only the SYN packets are received at the victim site from different IP addresses**.** The IP addresses are unreachable from the victim VM that lead to premature termination of the TCP connections at the server site. The victim resources are exhausted to analyse the IP addresses of the incoming SYN packets.

3.2.2.3 IP Spoofing with Offline VM

The attacker floods the TCP SYN packets with the spoofed IP addresses of other co-existing VMs that are offline at that instant.

The command used to flood TCP SYN request is:

sudo hping3 -flood -S -p 3000 192.168.43.138 – a 192.168.43.131

sudo hping3 -flood -S -p 3000 192.168.43.138 – a 192.168.43.134

-a: Specifies the spoofed IP address

The packet sequence is graphically shown by Flow Graph. In a short period of time there are number of SYN requests by the IP 192.168.43.131 and 192.168.43.134 to the VM 192.168.43.138. Within the Data Link Layer of the TCP/IP protocol stack,Address Resolution Protocol (ARP) is used convert IP

addresses to Media Access Control (MAC) addresses, within a private network When the VM wants to send data to the co–existing VM, ARP cache is used to find out the MAC address corresponding to the VM.

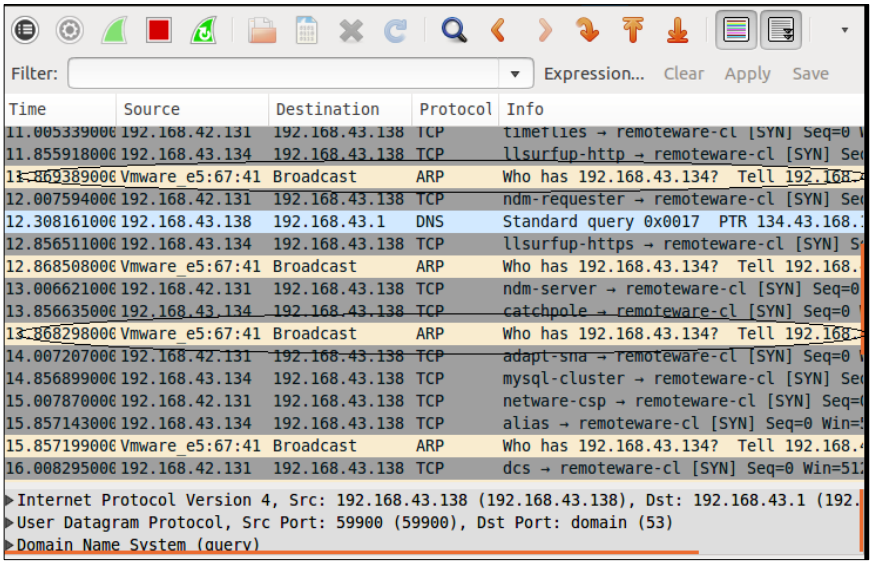

Figure 3.9: ARP Command to resolve the MAC

The victim VM tried to resolve the MAC address of the VMs (offline) as seen in the packet. But when no response is received by the offline VMs, the victim VM not having the MAC address (physical address) of the VMs, it cannot send an ACK-SYN to the same to continue with the three-way handshaking. The TCP/IP stack waits for the ARP requests.

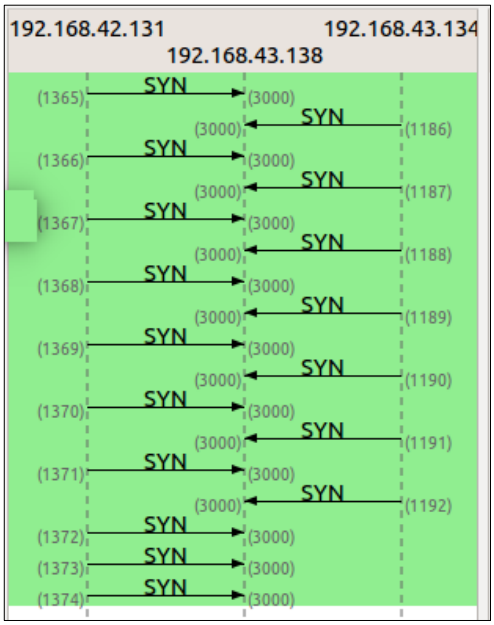

Figure 3.10: SYN Flood with Offline VM Spoofing

At the victim VM side, for each incoming SYN request, a memory called TCB (Transmission Control Block) is formed. The Transmission Control Block (TCB) is a data structure that holds all the data about the TCP connections. The TCB holds the SYN packet information before the connection is fully established. It holds only the half opened connection. The attacker floods the SYNs that causes so many Transmission Control Blocks allocation and victim VM's kernel memory is exhausted.

3.2.2.4 IP Spoofing with Online VM

The attacker VM sends SYN packets to the victim VM, with the spoofed IP addresses of the VM that are online on the same network. The spoofed VMs act as zombie. The zombie VM won't be expecting the SYN/ACK (because, it has not really sent the SYN), so the zombie VM responds to the victim VM with a RST. The victim VM's resources are depleted; it is not further create new TCP sessions legitimate network traffic.

The command used to flood TCP SYN request is:

sudo hping3 -flood -S -p 3000 192.168.43.138 – a 192.168.43.130

sudo hping3 -flood -S -p 3000 192.168.43.138 – a 192.168.43.132

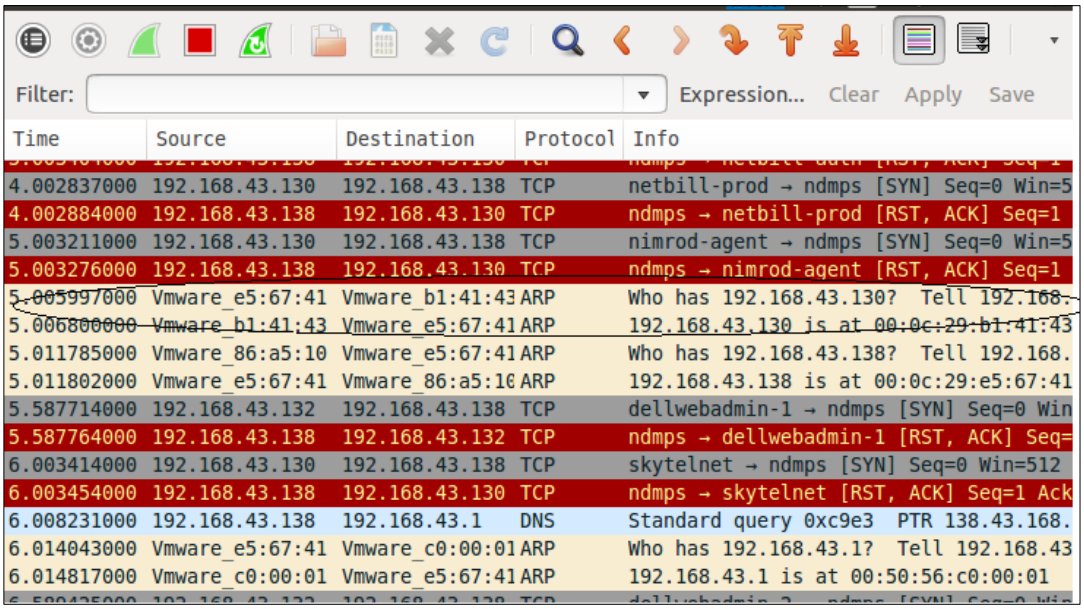

Figure 3.11: ARP Reply by online VMs

As the figure 3.11 shows the attacker used the spoofed IP address 192.168.43.132 and 192.168.43.130 to flood the victim 192.168.43.138. The victim VM sends ARP request to know the MAC addresses of the incoming IP

addresses. The Zombie VMs 192.168.43.130 replies for the ARP request with their MAC addresses.

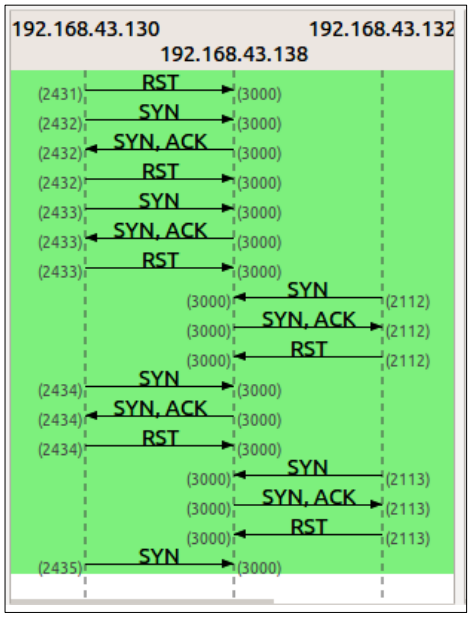

Figure 3.12: SYN Flood with Offline VM Spoofing

As the flow graph shows the victim VM sends the ACK-SYN packets to the respective IP addresses. As the Zombie VM has not sent the SYN packets, so it replied with the RST packet to the victim VM. The attacker keeps the victim busy in handling the spoofed packets and consuming the resources.

3.3 Defending the Denial of Service Attack

The firewalls are implemented at the hypervisor level and at the VM levels to prevent from internal network attack in the virtualized cloud infrastructure. The firewalls accept/deny the traffic according to the rules specified. The admin configures the firewalls at each virtual machine in the network. The traffic is to be intercepted by the VM before it reaches to it and TCP/IP packets are filtered, shaped and limited once a threshold has been reached.

3.3.1 Hypervisor Level Firewalls

Hypervisor is the main controlling agent for the virtual machines within the virtualization. The VMware ESXi hypervisor has its own security profile. The ESXi firewall is enabled that allows specific IP ranges to access a TCP service. The firewall resides in the core hypervisor kernel and monitors the virtual machine's incoming and outgoing traffic.

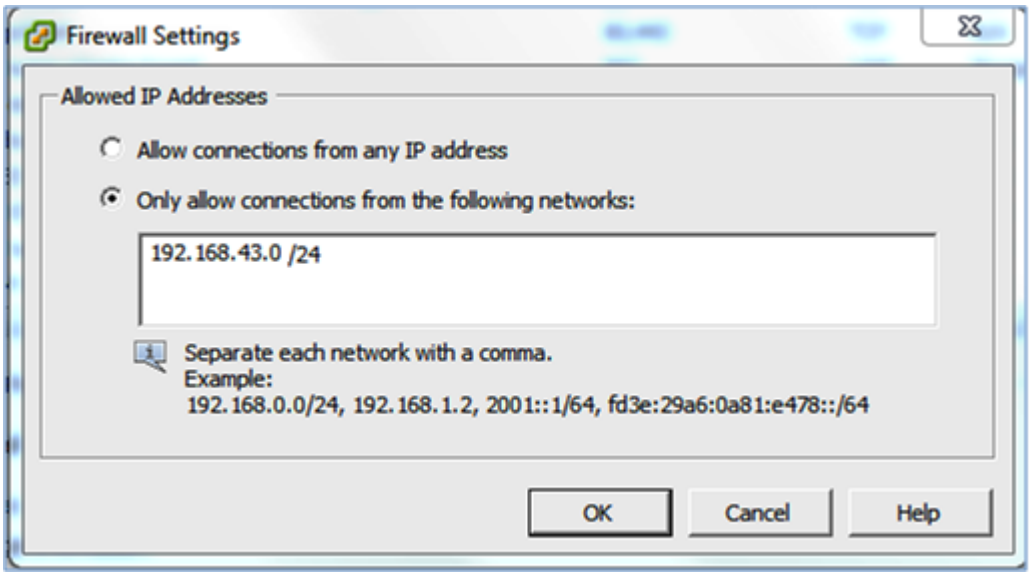

Figure 3.13: Hypervisor Firewalls

The hypervisor firewall isolates the internal network from the external network. When the malicious VM perform the TCP SYN Flood with random IP spoofing as shown in figure 3.8, the hypervisor firewall don't permit the random IP addresses generated by the attacker VM.

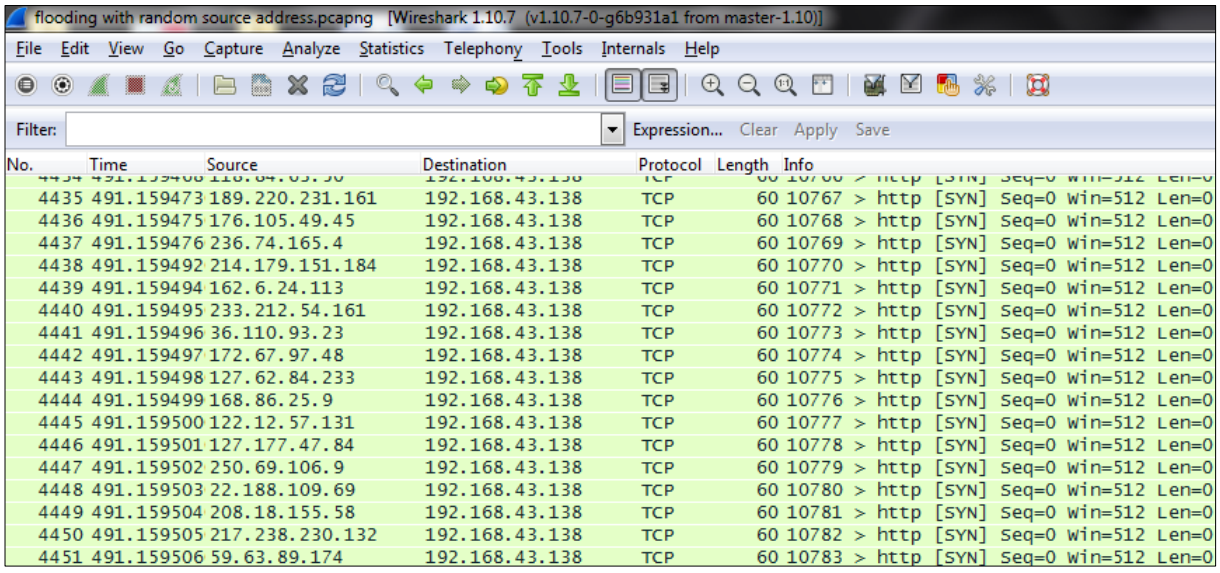

Figure 3.14: Dropping random spoofed packets

The victim VM don't broadcast the ARP request to resolve MAC address of random IP spoofed packets. The victim VM doesn't allocate TCB (Transmission Control Block) for the incoming SYN packets from random IP addresses and discard the packets. But the hypervisor firewalls can only prevent from the external

attacks. It doesn't prevent the DDoS attack when the malicious VM floods the victim VM with direct IP and subnet IP spoofing.

3.3.2 VM Level firewalls

To prevent from TCP SYN Flood attack by direct IP address and subnet IP spoofing, firewalls are configured at the VMs. A hybrid approach that combines Iptables firewalls and SYN cookies is used to defend the TCP SYN Flood attack at the victim virtual machine.

3.2.2.1 Iptables Firewalls

Itables firewalls uses IP addresses, protocols and ports to filter network traffic over the system. It keeps a stateful track of each connection passing through it.

A Shell script is written using IP tables to block TCP SYN Flood and limit the number of TCP connection request from an IP address. A threshold limit is configured that the co-existing VM can send maximum 30 SYN packetswithin one-second intervals. The packets are dropped if the limit exceeds. Additional firewall rules to prevent port scanning by the co-existing VM and rejecting spoofed packets is implemented (as shown in appendix A).

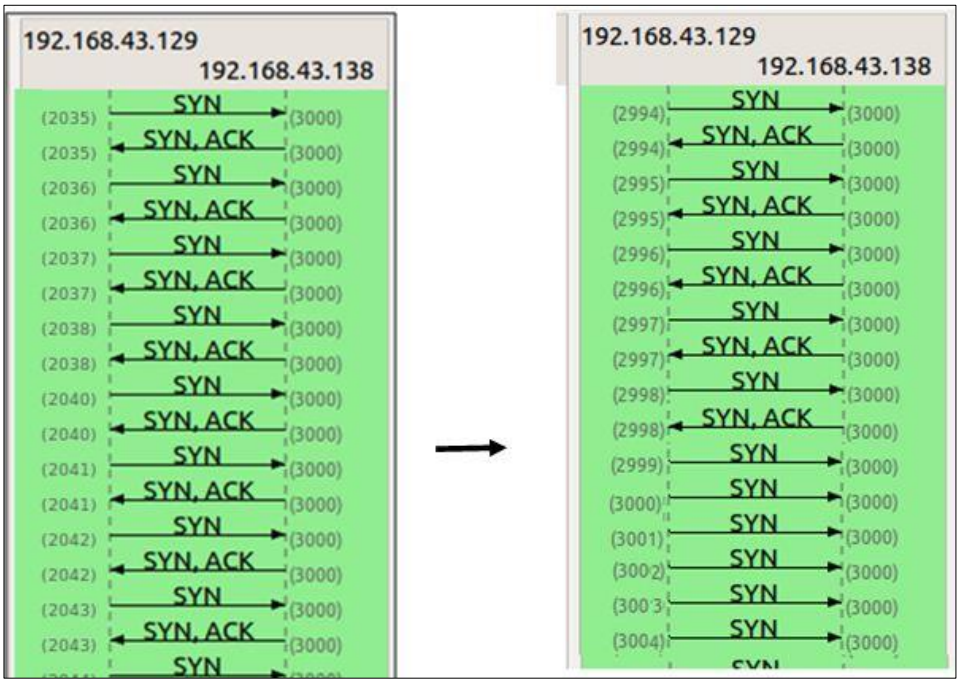

Figure 3.15: SYN Flood with own IP address

After blocking traffic using Iptables again capturing and analyzing of live traffic is done using wireshark.The attacker VM is sending SYN packets continuously to the VM after the threshold is reached the victim VM is not responding by sending SYN-ACK packets as all the packets are being dropped by the firewall according to the Iptables rules.

3.2.2.2 SYN_Cookies Protection

TheIptable firewalls don't fully block the denial of service attack; it has mitigated the impact of direct SYN flooding. Iptables don't provide security against subnet spoofed SYN flood as the online VMs reply with the RST packets and allocate TCB buffer for the offline VM to resolve the MAC address, To protect the victim VM from subnet spoofing (spoofed IP of online and offline VM) TCP_SYN cookies protection is enabled on the VM that validates the connection before allocating the resources. When the SYN segment request queue gets full, the kernel responds with a SYN-ACK packet that creates an encrypted sequence number that represents the source and destination IP address, the port and the timestamp of the received SYN request and validates the request before assigning the TCB.

To enable SYN cookies sysctl -w net.ipv4.tcp_syncookies=1 on the victim VM the file /etc/sysctl.conf is edited with the commands (shown in appendix B).

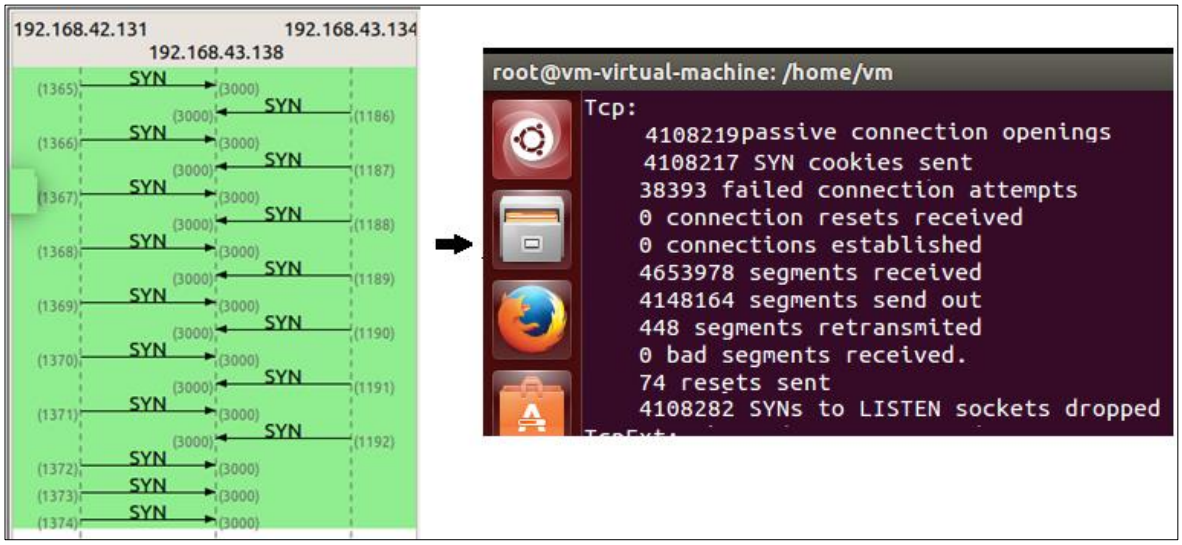

Figure 3.16: SYN Flood with offline VM

After enabling the SYN cookies traffic is captured again. The analyzing of Traffic is shows that SYN cookies don't allocate the TCB (Transmission control

block) as the SYN RCVDstate on reception of a SYN packet. The kernel replies directly with a SYN-ACK segment as SYN cookie and wait until the reception of a valid ACK. On receiving the valid ACK, the resources are allocated. The SYN cookies prevents the DDoS attack from IP spoofing with offline VMs.

To prevent the IP spoofing with online VM rp_filter of SYN_cookies is enabled that verifies the source route of packets, like unicast RPF (Reverse Path Forwarding) based on the source address of the packets.

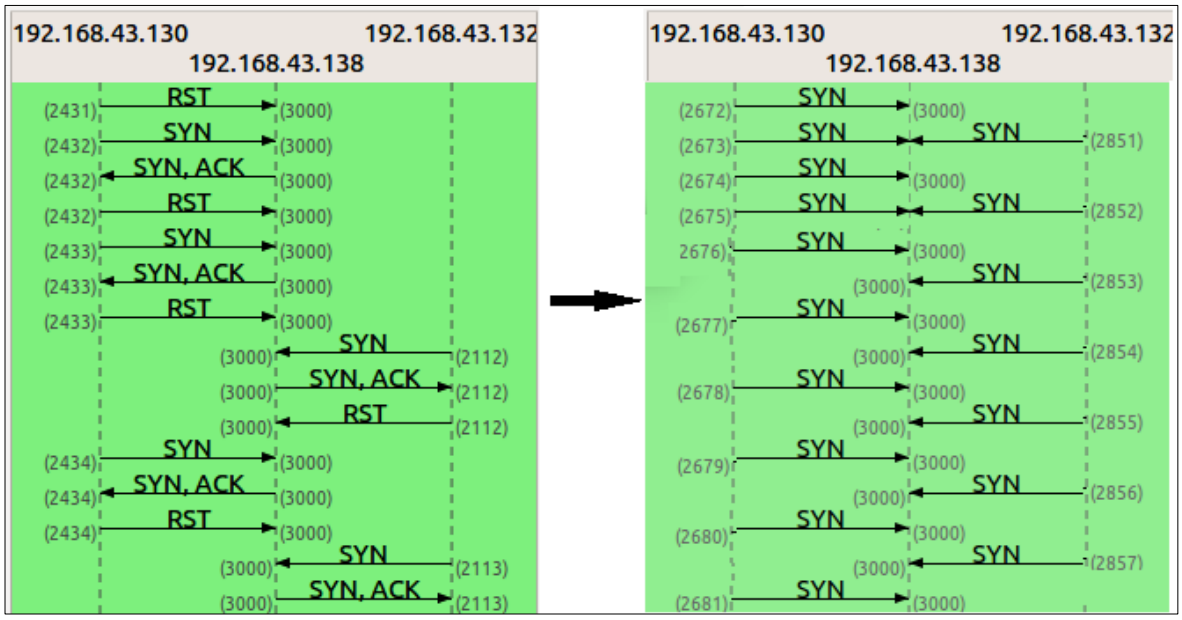

Figure 3.17: SYN Flood with online VM

The figure 3.17 depicts the difference between the packets capturing before the firewalls implemented and after that. The victim VM doesn't reply the spoofed SYN packets coming from malicious attacker VM.

The SYN flood attack exploits a vulnerability of the TCP three-way handshake. The implemented work shows how a malicious VM can exhaust the resources of the co-existing VM. The different kinds of SYN flooding attacks cause imbalance between the number of SYN packets and the SYN/ACK or FIN packets.Based on such imbalance the firewalls at the victim side are configured to block malicious traffic and protect legitimate traffic.

CHAPTER 4

RESULTS AND DISCUSSION

The chapter provides an analysis to the implemented research work in chapter 3. A variety of tools are employed in the research to detect the TCP-DDoS attack and to validate the performance of proposed model to mitigate the attack in the virtualized cloud. Wireshark, Netflow and IPtraf are few of the tools used to analyze the VM under attack. Exclusive Netstat commands are also used for getting the results. The performance of the victim VM under the attack is determined on the basis of network traffic, average number of SYN requests over the VM, number of half opened connections, OS response time, round trip etc.

4.1 Detection of TCP SYN Flood DDoS Attack on the Victim VM

In order to detect the presence of the attack various parameters are analyzed over the victim VM. Detection of the attack is done based on change in the network, protocol behavior from normal rates.

4.1.1 Number of SYN Requests Captured

The SYN packet is sent to initiate the TCP Three-way handshake. The attacker floods the victim VM by sending a large number of TCP SYN requests. Wireshark captures the SYN packet passing through the eth0 port .The Ethernet port was monitored during a TCP SYN flood attack.

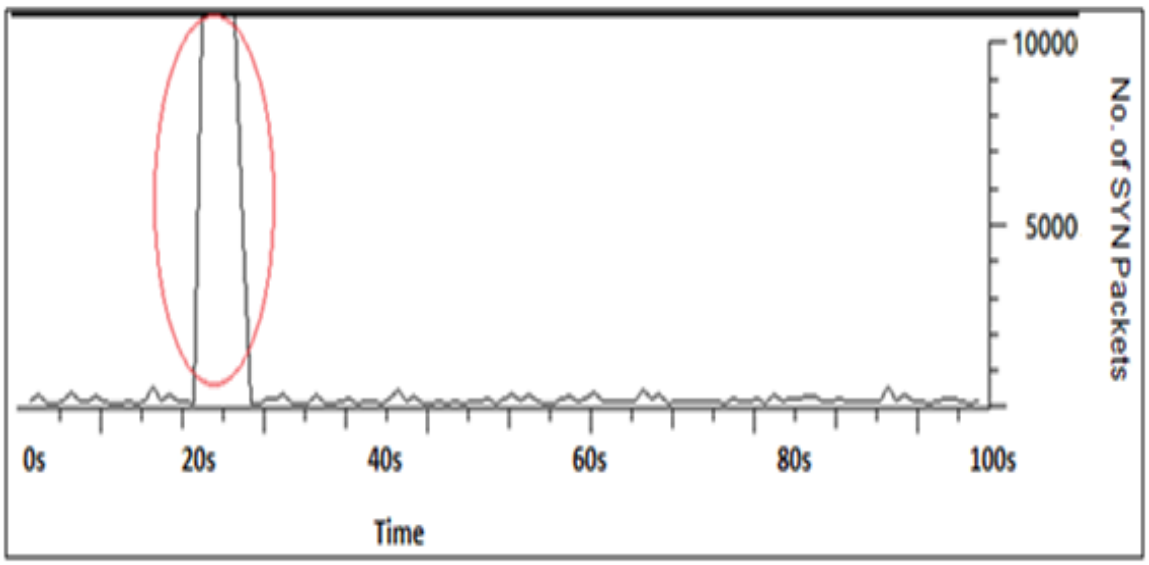

Figure 4.1: Number of SYN Packets at the victim VM with attack

The figure 4.1 shows the result of the incoming traffic for the TCP Port 3000. During TCP-SYN flood attack (from 20sec to 30sec) the number of SYN requests more than 10000 as compared to normal traffic that is about 5 to 10 SYN requests per second.

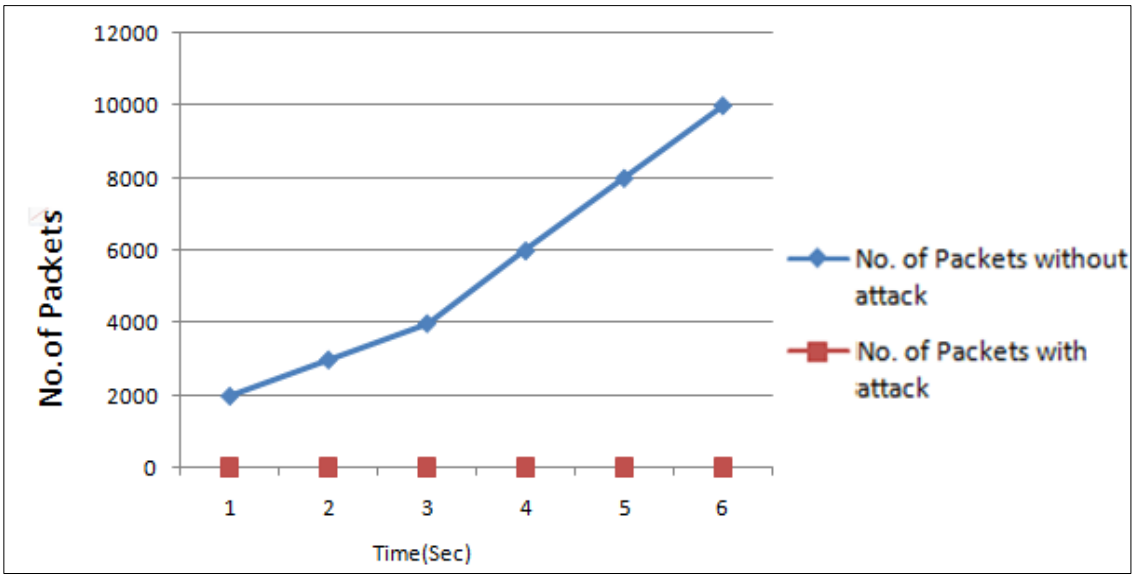

Figure 4.2: Number of SYN Packets with/without attack

The results have been compiled into a line graph which shows the number of packets on a machine with attack and without attack. By filtering the packets, the figure shows maximum 5 to 10 packets are captured per second at the network interface of the machine under the normal rate. The arrival rate of packets with TCP SYN flood attack is 5000 to 10000 packets per second. The analysis shows that at the time of attack the incoming rate of SYN packets increases at a very high rate.

4.1.2 SYN and FIN|RST Packet ratio.

TCP is a bi-directional protocol. The TCP connection is terminated by the FIN packet. The TCP connection performs half-duplex termination by sending RST packet from either side. The RST packet aborts the TCP connection. The number of FIN packets and the SYN packets are almost same under the normal TCP sessions. TCP session may be terminated by a RST packet without a FIN packet. But when the attack occurs, the relation between the SYN packets and FIN|RST Packets completely breaks. Detection of TCP SYN Flood is done based on the change of the difference between the number of SYN and the number of RST | FIN.

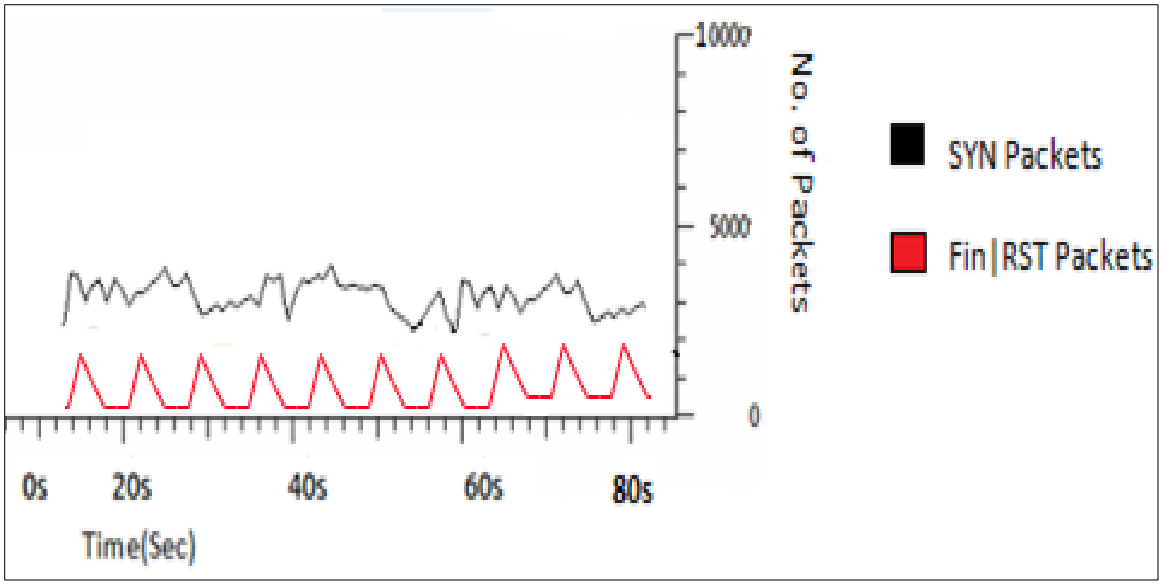

Figure 4.3: Normal SYN to FIN|RST packet rate

The figure 4.3 shows that the number of SYN and FIN|RST packets is almost same under normal network behaviour. The number of connections opened by the legitimate users is equal to the number of connections closed under the normal TCP session.

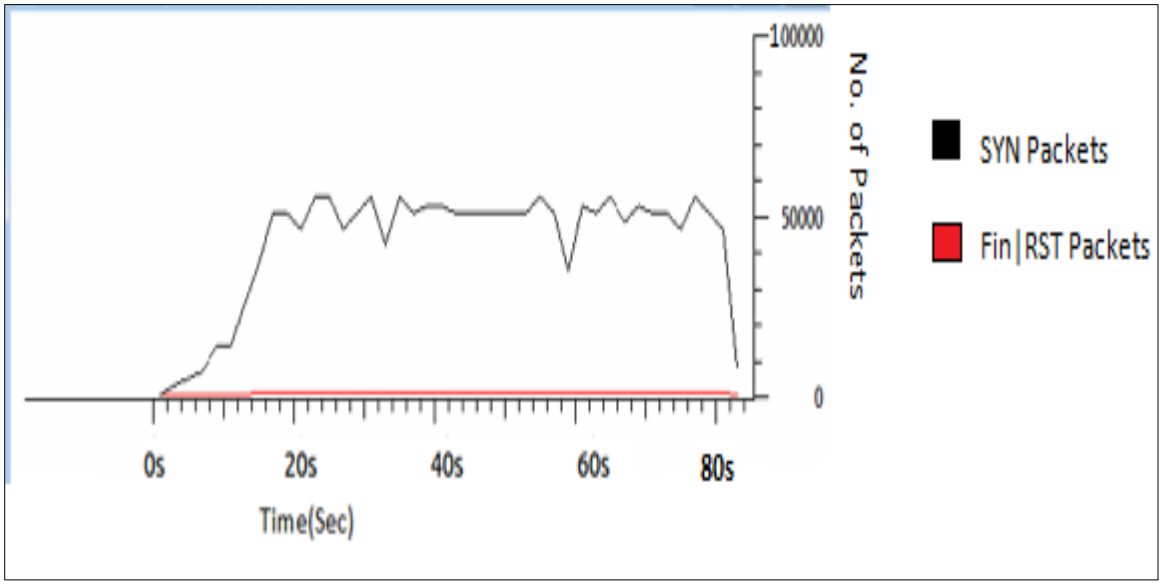

Figure 4.4: SYN to FIN|RST packet rate with SYN Flood

When the attacker performs the SYN Flooding to the VM, it doesn't terminate the connection at the victim VM side. Figure 4.4 shows the number of SYN and FIN|RST packets rate when the system is under attack. The number of SYN requests is very high as compared to the FIN|RST packet which is almost zero. The analysis shows that rate of SYN to FIN|RST packet is almost same

under the normal TCP sessions and at the time of attack number of FIN|RST packet is constantly Zero. The analysis shows that rate of SYN to FIN|RST packet is almost same under the normal TCP sessions and at the time of attack number of FIN|RST packet is constantly Zero.

4.1.3 The Start and End Time of an Attack

The exact time when the attack starts is analyzed with the post processing of the TCP SYN packets. Incoming traffic rate increases abruptly during the TCP SYN flood attack as compared to normal traffic rates.

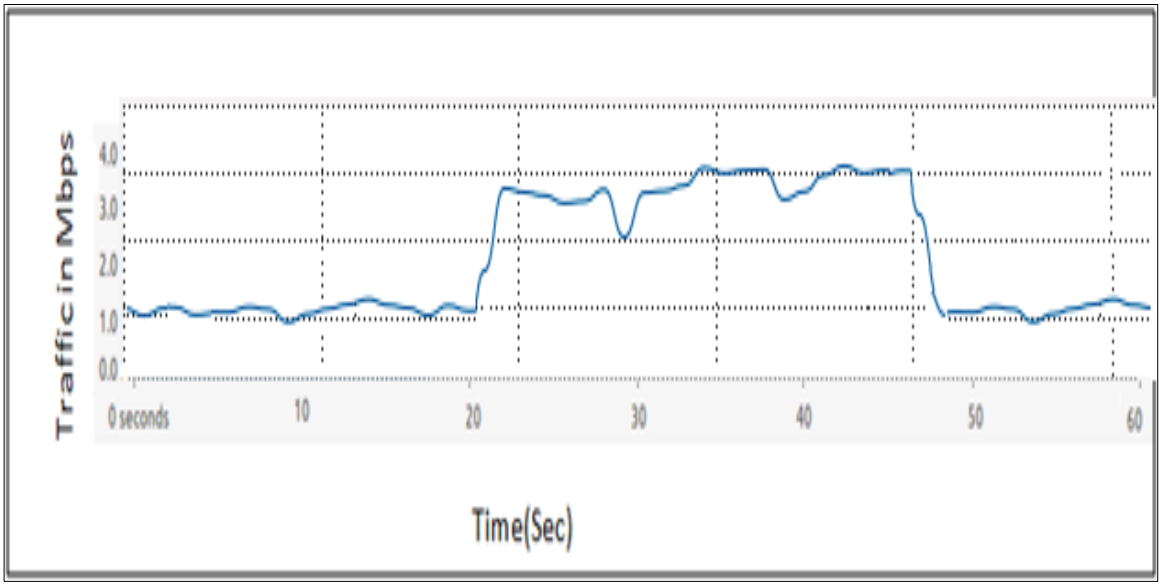

Figure 4.5: Time duration of attack

From the figure 4.5, it could be seen that the normal incoming traffic rate is almost 1 Mbps and the traffic rate goes up to 3Mbps at the time of TCP SYN flood attack from 20thsec to 50th sec. The SYN Flood attack is detected based on the incoming traffic rate that increases to 30% as compared to the traffic rates under normal network behavior.

4.1.4 RTT (Round Trip Time)

Round Trip Time is the time for TCP sessions from initial SYN packet to the ACK packet (third packet in the TCP three-way handshake).RTT is an important metric for a TCP connection. When a packet exceeds from its RTT value, the packet is considered to be lost and thus it is retransmitted in a TCP connection. Since retransmissions aggregates Denial of Service. During the TCP SYN Flood attack the packets are not acknowledged by the attacker.

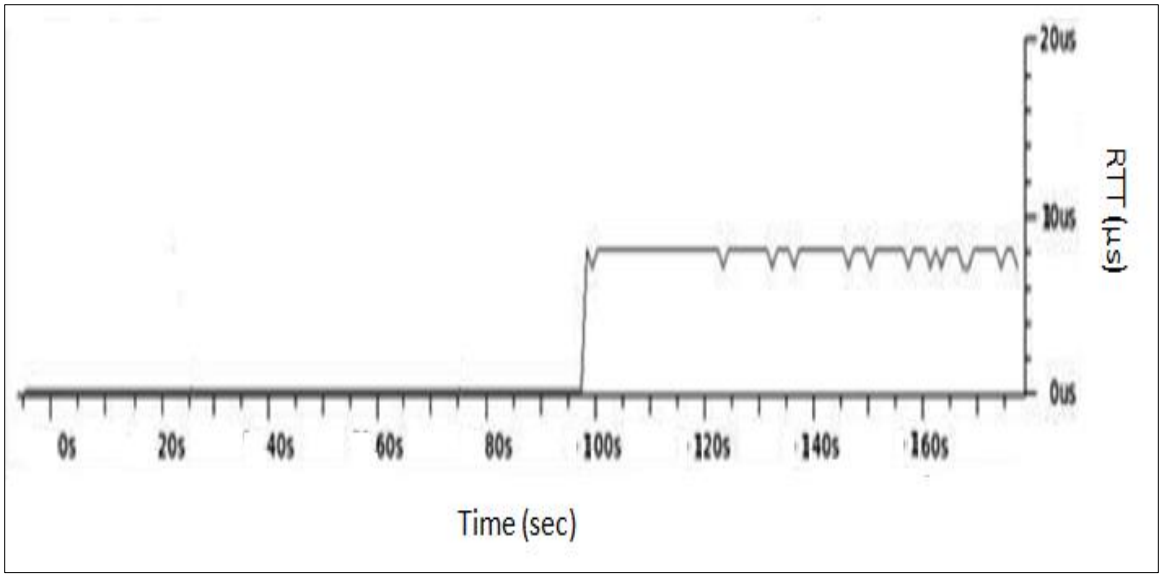

Figure 4.6: Round Trip Time of SYN Packets

The TCP RTT graph obtained at the victim VM under the TCP SYN Flood. When the attack is initiated, the round trip time increases to up to 10 microseconds as the attacker is not acknowledging the packets which stay almost constant till the attack is active. The analysis shows that at the time of attack the RTT increases to 10% at the time of attack.

4.2 Mitigation of the TCP DDoS Attack on the Victim VM

To evaluate the performance of the proposed model, the attacker virtual machine trying to communicate with the victim virtual machine. After starting with the normal communication, attacker VM starts sending attack traffic (TCP SYN Flood) to the victim VM at a very high rate. The attacker's virtual machine floods the victim at the maximum possible rate allowed by operating system. The TCP parameters are validated with a number of parameters with/without firewalls protection.

4.2.1 Response to the incoming SYN flood at the victim VM

The attacker's virtual machine floods the traffic at very high rate to the victim VM. The victim VM responses to the incoming traffic in order to establish the TCP connection. Without any firewalls protection VM is not cable to distinguish between the attacker's traffic and legitimate traffic. The victim VM sends the SYN-ACK packet to every incoming SYN request without firewalls packet filtering. The

attacker keeps the victim VM busy in handling the spoofed SYN requests and the VM is not able to communicate with the legitimate user.

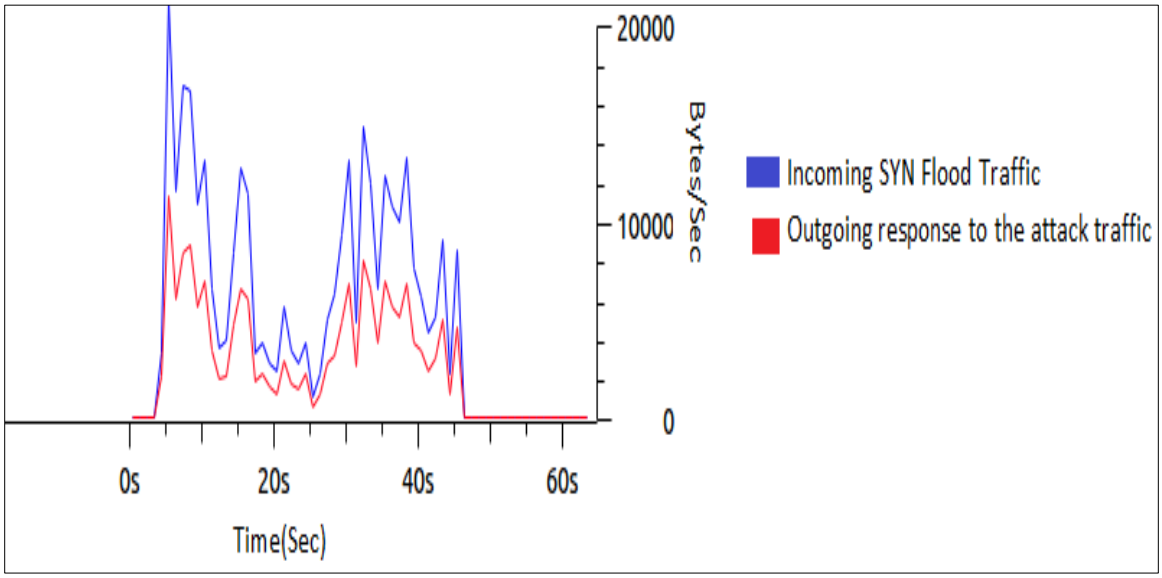

Figure 4.7: Response to the attack traffic without firewalls

The number of SYN packets at the victim side reaches to 10000. Without any firewalls protection, the victim VM, responses to TCP SYN packets. The outgoing traffic from the victim VM is shown through red lines in the figure 4.7.

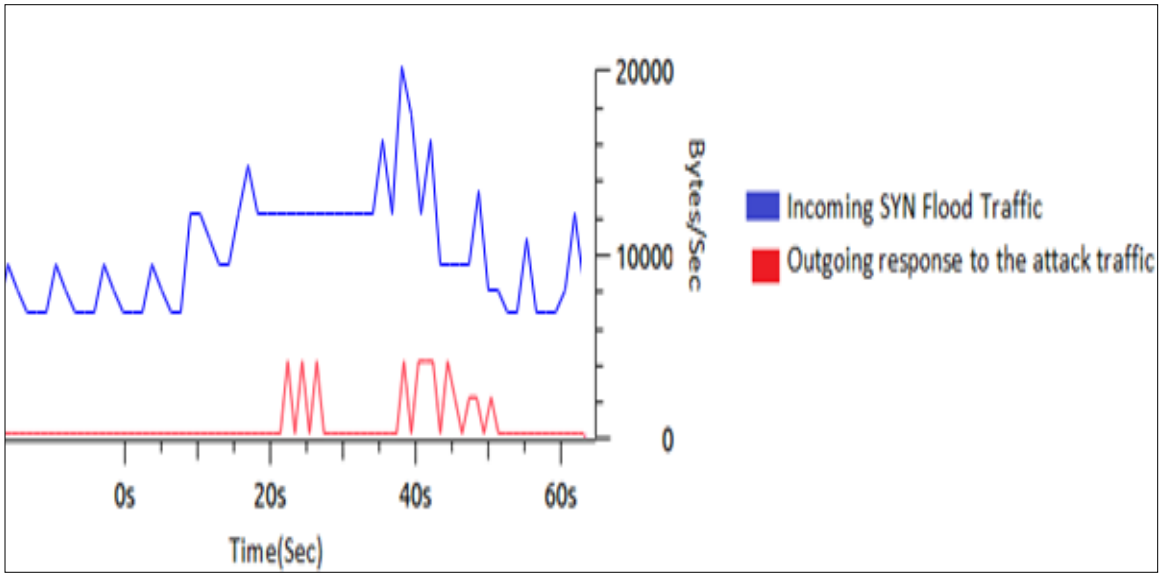

Figure 4.8: Response to the attack traffic without firewalls

The traffic captured after the firewalls implementation is shown in the figure 4.8. As the attacker is flooding the SYN Packets with the same rate as shown in figure 4.7, but the VM is not responding with the SYN-ACK with the same rate with

the firewall protection. The packets are dropped at the victim VM and the rate of outgoing packet reduces is shown through red lines.

Table 4.1: Number of SYN Packets at the victim VM attack with firewalls

	Incoming Traffic	outgoing Traffic
VM without Firewalls	15000(bytes per sec)$_{Approx}$	8000(bytes per sec)$_{Approx}$
VM without Firewalls	15000(bytes per sec)$_{Approx}$	200(bytes per sec)$_{Approx}$

It could be analyzed from the table 4.1 that the traffic rate considerably reduces from 8000bps to 200bps after applying mitigation strategies. The VM firewalls are able to reduce the traffic rate and prevent resources wastage at the victim.

4.1.3 Number of Half Opened Connections

The attacker leaves the TCP Three-way handshake half open by not sending the last ACK packet. Such half open state is stored in the memory of the VM and it keeps waiting for the final packet. When thousands of such half open connections are initiated, the VM runs out of its memory and crashes. It will not be able to serve the legitimate users as its memory is filled with attacker's requests.

Netstat tool is used to list all the inbound and outbound traffic connections over the victim VM from the terminal. The command used to list the number of active SYN connections is *"netstat* -nt**".**

```
root@vm-virtual-machine:/home/vm# netstat -nt
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.43.138:3000     192.168.43.129:47813    SYN_RECV
tcp        0      0 192.168.43.138:3000     192.168.43.129:10175    SYN_RECV
tcp        0      0 192.168.43.138:3000     192.168.43.129:47811    SYN_RECV
tcp        0      0 192.168.43.138:3000     192.168.43.129:10174    SYN_RECV
tcp        0      0 192.168.43.138:3000     192.168.43.129:45650    SYN_RECV
tcp        0      0 192.168.43.138:3000     192.168.43.129:39310    SYN_RECV
tcp        0      0 192.168.43.138:3000     192.168.43.129:979      SYN_RECV
tcp        0      0 192.168.43.138:3000     192.168.43.129:47815    SYN_RECV
tcp        0      0 192.168.43.138:3000     192.168.43.134:47812    SYN_RECV
tcp        0      0 192.168.43.138:3000     192.168.43.134:45649    SYN_RECV
tcp        0      0 192.168.43.138:3000     192.168.43.134:62826    SYN_RECV
tcp        0      0 192.168.43.138:3000     192.168.43.129:45648    SYN_RECV
tcp        0      0 192.168.43.138:3000     192.168.43.129:980      SYN_RECV
tcp        0      0 192.168.43.138:3000     192.168.43.131:47814    SYN_RECV
tcp        0      0 192.168.43.138:3000     192.168.43.131:62825    SYN_RECV
```

Figure 4.9: No of half opened connections without firewalls

The number of awaiting final SYN connection is more than 5000 during the TCP SYN attack without firewalls protection. It completely drains out the operating

system memory of the VM. The victim VM was not able to hold all the pending SYN connections in its CPU memory space and starts dropping the incoming legitimate requests.

```
root@vm-virtual-machine:/home/vm# netstat -nt
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.43.138:3000     192.168.43.131:1382     SYN_RECV
tcp        0      0 192.168.43.138:3000     192.168.43.131:1377     SYN_RECV
tcp        0      0 192.168.43.138:3000     192.168.43.131:1373     SYN_RECV
tcp        0      0 192.168.43.138:3000     192.168.43.131:1372     SYN_RECV
tcp6       1      0 ::1:47655               ::1:631                 CLOSE_WAIT
root@vm-virtual-machine:/home/vm#
```

Figure 4.10: No of half opened connections with firewalls

With the firewalls as the syn_cookies validates the connection before allocating the CPU memory. The Iptables firewall also limits the maximum number of connection per second. Figure 4.10 shows the number of half opened connections with VM firewalls which is negligible.

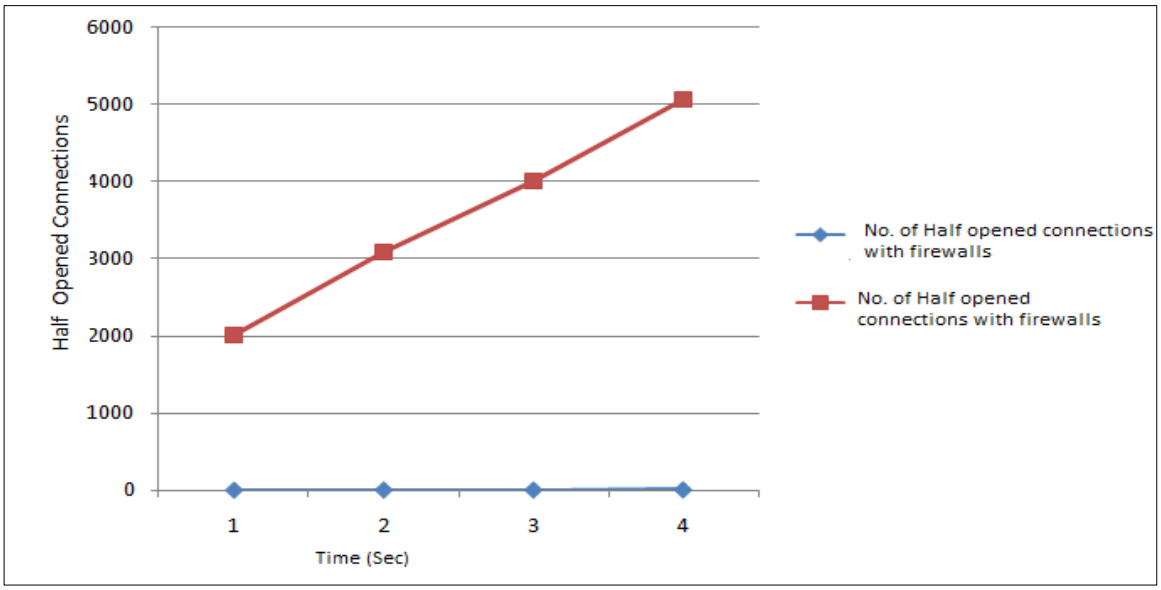

Figure 4.11: No. of half opened connections

The figure 4.11 shows the connection status. When there is no firewall protection at the victim at the initial stages of SYN flood attack, the number of active connection showed about 2000 and then increases up to 5000 during the peak. With the firewalls the number of half opened connections is very less that is 2 to 4.

4.1.4 CPU Utilization

CPU utilization refers to hypervisor's usage of processing resources. As under the virtualized cloud infrastructure the single CPU is shared among multiple VMs. The vSphere client gives the traffic details and CPU utilization for each virtual machine.

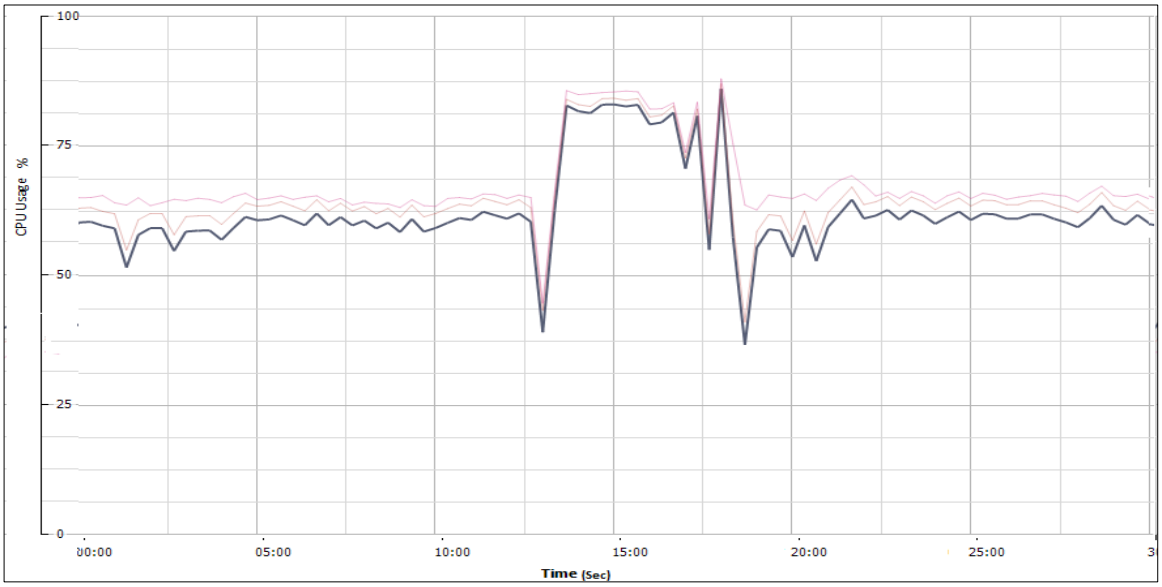

Figure 4.12: CPU Utilization

From the figure 4.12, it could be seen that CPU % utilization for the single victim virtual machine increases from 60 % to 90% when it is under the attack (15 sec to 20 sec) without firewall protection. The firewalls are enabled at the 20th second and percentage CPU utilization decreases to 50.

4.1.5 Memory utilization

For each TCP connection, that tries to be established, a queue is maintained in the memory that holds all the information about a TCP connection. The queue holds the SYN packet information before the connection is fully established. It holds only the half opened connections. During the TCP SYN Flood attack a large number of half-opened connections are left at the victim site so that VM's kernel memory is exhausted.

The vSphere client also details the memory utilization for each virtual machine. CPU memory is utilized to store the incoming packets information until TCP session is not completed.

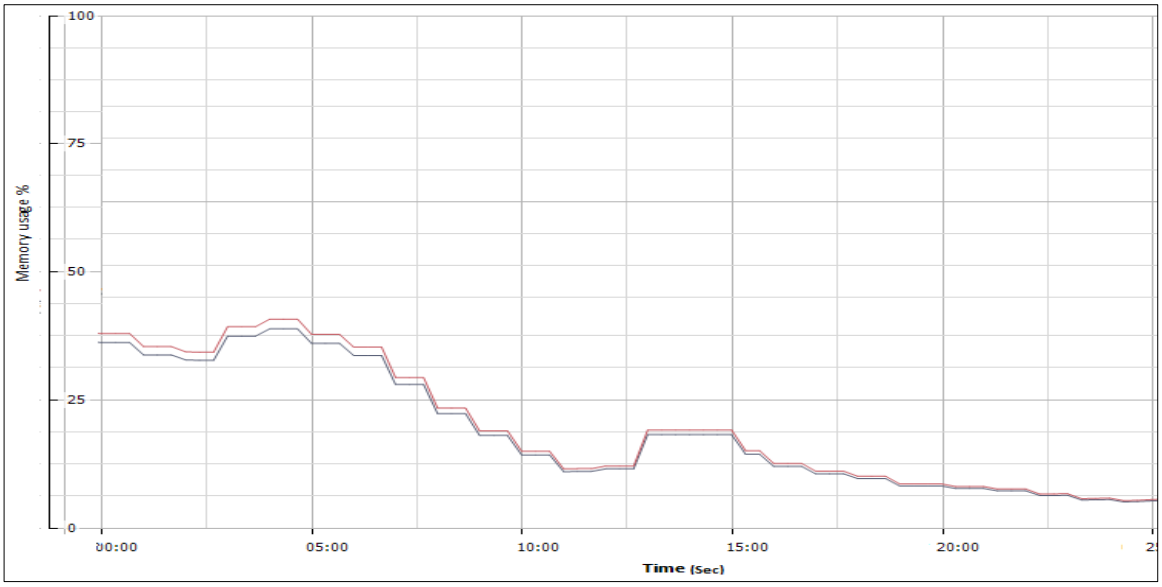

Figure 4.13: Memory Utilization

During the TCP SYN Flood attack memory % utilization for the single victim virtual machine increases upto 50% (upto 7th Sec) without firewall protection. The firewalls are enabled at the victim (8th sec to until) memory utilization decreases to 20%.

From the above it could be concluded that when there is a malicious virtual machine present in the virtualized cloud, it could be detected on the basis of different parameters over the victim operating system. The network traffic over the VM increases at a very high rate as compared to average traffic rates. The firewalls presence at the virtual machine distinguishes the legitimate traffic from the attacker's traffic and improves the overall performance of the virtualized cloud environment.

CHAPTER 5
CONCLUSIONS AND FUTURE SCOPE

Security of the virtual network is the most significant concern in the cloud platform. Cloud computing has multiple service and deployment models with their own security concerns. The dissertation focuses on private IaaS clouds, where the tenants are more vulnerable to attacks. The use of the virtualization is to isolate all the co-resident VMs under the hypervisor. But there are various kinds of security breaches in the virtualization which violates the isolation between various VMs.

The research provides an overview of cloud computing, including multi-tenant architecture and virtualization technologies. The work focused on the various kinds of attacks and vulnerabilities associated with virtualization in the cloud computing. Vulnerabilities of TCP–DDoS attack over the Host Machine in the cloud is analyzed in the simulated environment. The dissertation demonstrates the ways how a malicious VM can perform the Distributed Denial of Service attack over other co-existing VM in the virtualized cloud. The work explores the sensitivity of virtualization in the cloud and provides measures to secure it from DDoS attack.

- **Detection of DDoS attack:** The parameters network traffic are analyzed and validated at the victim and the results showed that the arrival rates of normal TCP SYN packets and attacked SYN Flood varies with large difference. On the basis of daily network behaviour a SYN Packet arrival rate is decided. The presence of TCP-DDoS attack is determined based on the average number of SYN requests in the VM, SYN to FIN|RST packet ratio.
- **Mitigation of DDoS Attack:** Capabilities of the firewalls at the hypervisor level and the VM level is explored, to defend against the DDoS attack. To determine whether the network traffic is legitimate or not, the virtual machine not only relies on the hypervisor firewalls. A firewall to mitigate the effect of direct SYN Flood and subnet IP Spoofing attack is also configured at the virtual machine side. The firewall rules refine the legitimate traffic over the victim virtual machine.

- **Enhance the isolation between VMs**: The firewalls configured over the virtual machines increases the virtual machine security in the virtualized cloud.

The VM level firewalls have prevented the virtual machines from the internal attacks by the co-existing malicious virtual machine.

Future Scope

The work presented in the dissertation can be pursued with various research directions to make the virtualized cloud more secure.

- The research can be extended to validate the model with other IaaS platforms.
- Another active area of research could be to secure the virtualized cloud from other kinds of internal attacks.
- The firewall strategies can be further improved to defend the attacks not limited to TCP-DDoS.

REFERRENCES

Bakshi, A. and Yogesh, B. (2010). Securing cloud from ddos attacks using intrusion detection system in virtual machine. In Proceedings of the Second International Conference on Communication Software and Networks. pp. 260-264. Singapore.

Bamiah, M. A. and Brohi, S. N. (2011). Seven deadly threats and vulnerabilities in cloud computing. International Journal of Advanced Engineering Sciences and Technologies. 9**(1)**: 87-90.

Brohi, S. N. Bamiah, M. A. Brohi, M. N. and Kamran, R. (2012). Identifying and analyzing security threats to Virtualized Cloud Computing Infrastructures. In Proceedings of the International Conference on Cloud Computing Technologies, Applications and Management. pp. 151-155. Dubai.

Brunette, G. and Mogull, R. (2009). Security guidance for critical areas of focus in cloud computing v2. 1. Cloud Security Alliance. 1-76.

Buyya, R. Broberg, J. and Goscinski, A. M. (2010). Cloud computing: Principles and paradigms. John Wiley & Sons. New York.

Choi, Y. S. Oh, J. T. Jang, J. S. and Ryou, J. C. (2010, August). Integrated DDoS attack defense infrastructure for effective attack prevention. In Proceedings of the 2nd International Conference on Information Technology Convergence and Services. pp. 1-6. Cebu.

Dawoud, W. Takouna, I. and Meinel, C. (2010). Infrastructure as a service security: Challenges and solutions. In Proceedings of the The 7th International Conference on Informatics and Systems. pp. 1-8. Cairo.

Eddy, W. M. (2006). Defenses against TCP SYN flooding attacks. The Internet Protocol Journal. 9**(4):** 2-16.

Hao, F. Lakshman, T. Mukherjee, S. and Song, H. (2010). Secure cloud computing with a virtualized network infrastructure. In Proceedings of the 2nd USENIX conference on Hot topics in cloud computing. pp. 16-16. USENIX Association Berkeley, CA, USA.

Hwang, J. Zeng, S. and Wood, T. (2013, May). A component-based performance comparison of four hypervisors. In Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management. pp. 269-276. Ghent.

Jamsa, K. (2013). Cloud computing. Jones & Bartlett Publishers.

Jansen, W. and Grance, T. (2011). Guidelines on security and privacy in public cloud computing. NIST special publication 800-144.

Jasti, A. Shah, P. Nagaraj, R. and Pendse, R. (2010, October).Security in multi-tenancy cloud. In Proceedings of the International Carnahan Conference on Security Technology. pp. 35-41. San Jose, CA.

Kalagiakos, P. and Bora, M. (2012, October). Cloud security tactics: Virtualization and the VMM. In Proceedings of the 6th International Conference on Application of Information and Communication Technologies. pp. 1-6. Tbilisi.

Kavisankar, L. and Chellappan, C. (2011, June). A Mitigation model for TCP SYN flooding with IP Spoofing. In Proceedings of the International Conference on Recent Trends in Information Technology. pp. 251-256. Chennai, Tamil Nadu.

Mather, T. Kumaraswamy, S. and Latif, S. (2009). Cloud security and privacy: an enterprise perspective on risks and compliance. " O'Reilly Media, Inc.".

Mell, P. and Grance, T. (2011). The NIST definition of cloud computing. NIST special publication 800-145.

Mirzaie, S. Elyato, A. K., and Sarram, M. A. (2010, February). Preventing of SYN Flood attack with iptables Firewall. In Proceedings of the Second International Conference on Communication Software and Networks. pp. 532-535. Singpore.

Nomnga, P. Scott, M. S. Nyambi,and P. B. A. (2014) Technical Cost Effective Network-Domain Hosting through Virtualization: a VMware ESXi and vSphere Client Approach. International Journal of Computer Applications. 91**(10):** 30-47.

Nazri, M. I. Aborujilah, A. Musa, S. and Shahzad, A. (2012). New Framework to Detect and Prevent Denial of Service Attack in Cloud Computing Environment. International Journal of Computer Science and Security. 6**(4):** 226-237.

Reuben, J. S. (2007). A survey on virtual machine security. Seminar on Network Security. Helsinki University of Technology.

Rhoton, J. (2009). Cloud Computing Explained: Implementation Handbook for Enterprises. Recursive Press Pages.

Sabahi, F. (2011a). Virtualization-level security in cloud computing. In Proceedings of the 3rd International Conference on Communication Software and Networks. pp. 250-254.

Sabahi, F. (2012b). Secure Virtualization for Cloud Environment Using Hypervisor-based Technology. International Journal of Machine Learning and Computing. 2**(1):** 30-25.

Schuba, C. L. Krsul, I. V. Kuhn, M. G. Spafford, E. H. Sundaram, A. and Zamboni, D. (1997, May). Analysis of a denial of service attack on TCP. In Proceedings of the IEEE Symposium on Security and Privacy. pp. 208-223. Oakland, CA.

Shea, R. and Liu, J. (2012a). Understanding the impact of denial of service attacks on virtual machines. In Proceedings of the 20th International Workshop on Quality of Service. pp 1-7. Coimbra.

Shea, R. and Liu, J. (2013b). Performance of Virtual Machines under Networked Denial of Service Attacks: Experiments and Analysis. Systems Journal. IEEE. 7**(2):** 335-345.

Soundararajan, V. and Govil, K. (2010). Challenges in building scalable virtualized datacenter management. ACM SIGOPS Operating Systems Review. 44**(4):** 95-102.

Subashini, S. and Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications. 34**(1):** 1-11.

Szefer, J. and Lee, R. B. (2011, June). A case for hardware protection of guest vms from compromised hypervisors in cloud computing. In Proceedings of the 31st International Conference on Distributed Computing Systems Workshops. pp. 248-252.

Turnbull, L. and Shropshire, J. (2013, April). Breakpoints: An analysis of potential hypervisor attack vectors. In Proceedings of IEEE. pp. 1-6. Southeastcon.

Velte, T. Velte, A. and Elsenpeter, R. (2009).Cloud computing, a practical approach. McGraw-Hill, Inc.

Wang, H. Zhang, D. and Shin, K. G. (2002, June). Detecting SYN flooding attacks. In Proceedings of the Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. pp. 1530-1539. New York, USA.

Wang, H. Zhang, D. and Shin, K. G. (2004). Change-point monitoring for the detection of DoS attacks. IEEE Transactions on Dependable and Secure Computing. 1**(4):** 193-208.

Wei, Z. Xiaolin, G. Wei, H. R. and Si, Y. (2012, May). TCP DDOS attack detection on the host in the KVM virtual machine environment. In Proceedings of the 11th International Conference on Computer and Information Science. pp. 62-67.

Wesley, M. E. (2006). Defences against TCP SYN Flooding Attacks. The Internet Protocol Journal. 9**(4):** 1-5.

Wu, H. Ding, Y. Winer, C. and Yao, L. (2010). Network security for virtual machine in cloud computing. In Proceedings of the 5th International Conference on Computer Sciences and Convergence Information Technology. pp. 18-21.

Zuquete, A. (2002). Improving the functionality of SYN cookies. In Proceedings of the International Conference on Advanced Communications and Multimedia Security. pp. 57-77. Springer US.

APPENDIX-A

IPTABLES FIREWALLS

```
#!/bin/sh

# flushing the iptables
IPTABLES -F
IPTABLES -X
IPTABLES -Z

# dropping everything by default
IPTABLES -P INPUT DROP
IPTABLES -P FORWARD DROP
IPTABLES -P OUTPUT DROP

# Allowing loopback interface
IPTABLES -A INPUT -i lo -j ACCEPT
IPTABLES -A OUTPUT -o lo -j ACCEPT


# Allowing incoming connections related to existing allowed connections.
IPTABLES -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT


# Allowing outgoing connections EXCEPT invalid
IPTABLES -A OUTPUT -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
IPTABLES -A INPUT -p tcp --tcp-flags ALL FIN,URG,PSH -j DROP
IPTABLES -A INPUT -p tcp --tcp-flags SYN,RSTSYN,RST -j DROP
IPTABLES -A INPUT -p tcp --tcp-flags SYN,FINSYN,FIN -j DROP


# Dropping invalid incoming traffic
IPTABLES -A INPUT -m state --state INVALID -j DROP


# Dropping invalid outgoing traffic.
IPTABLES -A OUTPUT -m state --state INVALID -j DROP


# Dropping Spoofed Packets
IPTABLES -A INPUT -i eth0 -s 0.0.0.0/8 -j DROP
IPTABLES -A INPUT -i eth0 -s 127.0.0.0/8 -j DROP
IPTABLES -A INPUT -i eth0 -s 10.0.0.0/8 -j DROP
IPTABLES -A INPUT -i eth0 -s 172.16.0.0/12 -j DROP
IPTABLES -A INPUT -i eth0 -s 224.0.0.0/3 -j DROP
```

```
# Dropping the new connection if it is not SYN
IPTABLES -A INPUT -p tcp ! --syn -m state --state NEW -j DROP

# SYN-flood protection
IPTABLES -N SYN-FLOOD
IPTABLES -A INPUT -p tcp --SYN -J SYN-FLOOD
IPTABLES -A SYN-FLOOD -m limit --limit 30/s --limit-burst 60 -J RETURN
IPTABLES -A SYN-FLOOD -J LOG --LOG-LEVEL 4 --LOG-PREFIX 'SYN-FLOOD ATTEMPT: '
IPTABLES -A SYN-FLOOD -J DROP

# Setting SYN Flood countermeasures
IPTABLES -A INPUT -m state --state NEW -p tcp -m tcp --syn  -m recent --name synflood --set
IPTABLES -A INPUT -m state --state NEW -p tcp -m tcp --syn  -m recent --name synflood --update --seconds 1 --hitcount 60 -j DROP

# Blocking the scan for open ports
IPTABLES -A INPUT   -p tcp -m tcp --dport3000  -m recent --name portscan --set -j LOG --log-prefix "Portscan"
IPTABLES -A INPUT    -p tcp -m tcp --dport 3000 -m recent --name portscan --set -j DROP
IPTABLES -A FORWARD -p tcp -m tcp --dport3000  -m recent --name portscan --set -j LOG --log-prefix "Portscan"
IPTABLES -A FORWARD -p tcp -m tcp --dport 3000 -m recent --name portscan --set -j DROP

# END
```

APPENDIX-B

ENABLING SYN COOKIES ON THE VICTIM VM

sudo vi /etc/sysctl.conf (To edit /etc/sysctl.conf file)

```
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables
# See sysctl.conf (5) for information.
#
# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.all.rp_filter = 1
# Uncomment the next line to enable TCP/IP SYN cookies
net.ipv4.tcp_syncookies = 1
net.ipv4.tcp_max_syn_backlog = 2048
net.ipv4.tcp_synack_retries = 2
net.ipv4.tcp_syn_retries = 5


# Do not accept ICMP redirects (prevent MITM attacks)
# net.ipv4.conf.all.accept_redirects = 0
# net.ipv6.conf.all.accept_redirects = 0
# net.ipv4.conf.default.accept_redirects = 0
# net.ipv6.conf.default.accept_redirects = 0
```

```
# Do not send ICMP redirects (we are not a router)
# net.ipv4.conf.all.send_redirects = 0
# net.ipv4.conf.default.send_redirects = 0

# Do not accept IP source route packets (we are not a router)
# net.ipv4.conf.all.accept_source_route = 0
# net.ipv6.conf.all.accept_source_route = 0
# net.ipv4.conf.default.accept_source_route = 0
# net.ipv6.conf.default.accept_source_route = 0

# Log Martian Packets
# net.ipv4.conf.all.log_martians = 1
# net.ipv4.icmp_ignore_bogus_error_responses = 1

# Ignore ICMP broadcast requests
# net.ipv4.icmp_echo_ignore_broadcasts = 1

# Ignore Directed pings
net.ipv4.icmp_echo_ignore_all = 1
```

sysctl –p (To save the changes)

APPENDIX-C

INSTALLATION STEPS OF VMware ESXi HYPERVISOR AND VIRTUAL MACHINES

Minimum System Requirements for the installation are:

Table C.1: Installation Requirements

Processor	64-bit x86 CPUs with at least two cores.
RAM	2GB RAM minimum.
Hard Disk Space	10GB minimum
Network Adapters	One or more Gigabit or 10Gb Ethernet controllers

First step is to register on VMware portal to download vSphere hypervisor (ESXi). After the registration VMware allows to download VMware ESXi 5.0 iso and issues serial key for ESXi.

1. The VMware Workstation 9 is installed over the windows 7 to run VMare ESXi 5.0 as a virtual machine. On VMware Workstation home page, go to the File menu and click on New Virtual Machine.

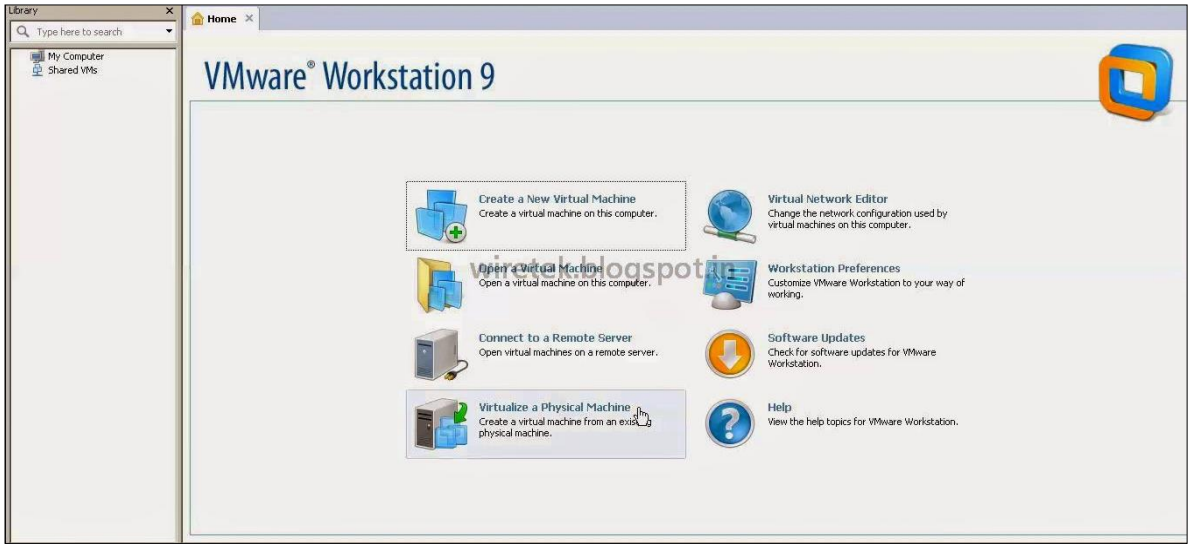

Figure C.1: VMware Workstation Console

2. The New Virtual Machine Wizard opens and allows choosing Typical or Custom configuration for new VM. Choose Custom configuration and click Next.

Figure C.2: Configuration Type for New VM

3. To choose hardware compatibility for VMs. It is set to Workstation 9.0. Click Next.

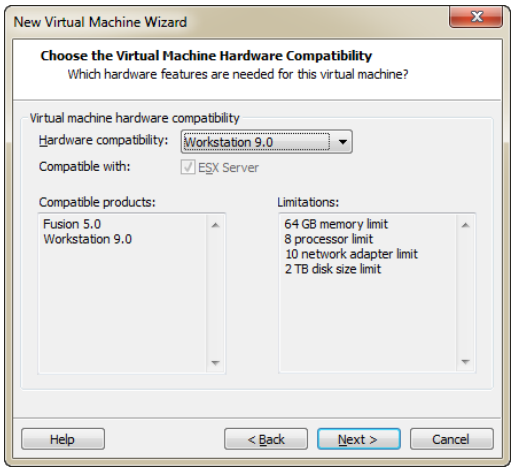

Figure C.3: Hardware compatibility

4. Browse the VMware ESXi iso. VMware Workstation automatically detects VMware ESXi 5. All the other options needed for the installation are automatically recommended by the VMware workstation. Click Next to proceed.

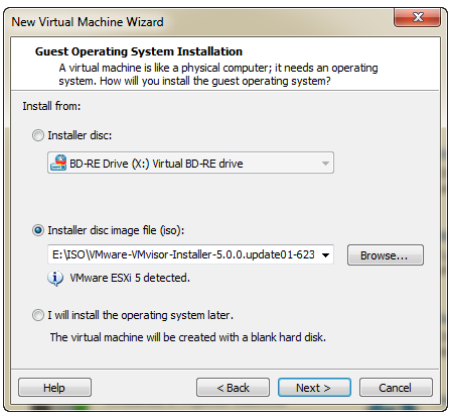

Figure C.4: VMware ESXi iso

5. The memory needed to the VMware ESXi hypervisor recommended by the workstation is from 2 GB to 16 GB. For the research work, 4 GB is selected.

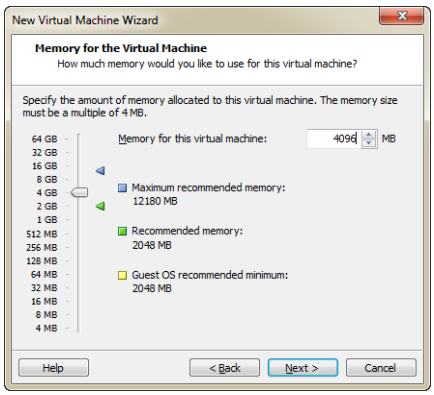

Figure C.5: Memory Allocation to VMware ESXi

6. Disk space needed for the VMware ESXi is 10 GB to 40 GB. 40 GB is selected**.** Then click Next to proceed.

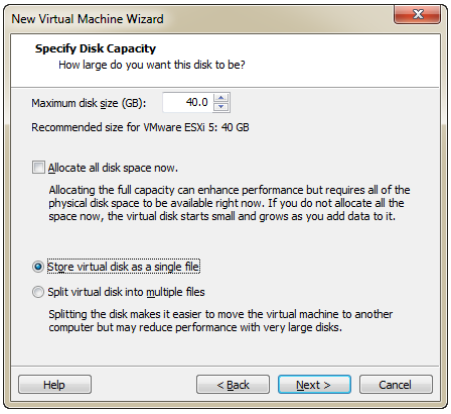

Figure C.6: Disk Space Allocation to VMware ESXi

7. Click Finish and virtual machine starts. After some time the installer starts loading.

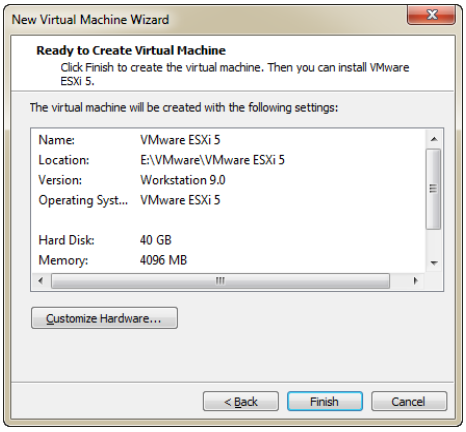

Figure C.7: ESXi VM

8. ESXi 5 iso image continues to boot.

Figure C.8: ESXi ISO Booting

9. Press F11 to accept the End User License Agreement.

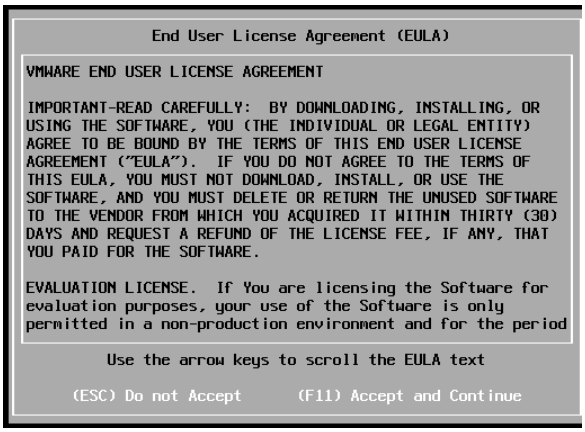

Figure C.9: License Agreement

10. Enter the root password. Press enter.

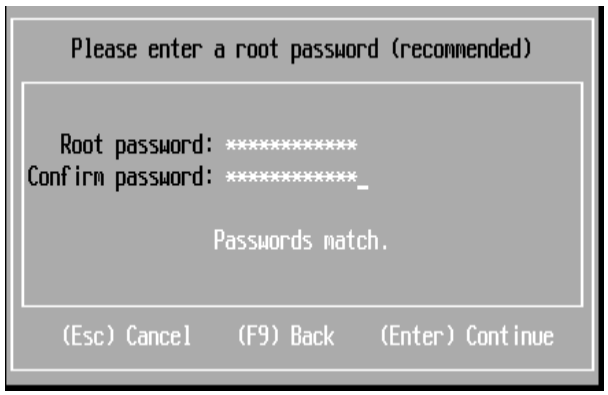

Figure C.10: The ESXi Hypervisor Password

11. After the installation is complete, it is required to reboot the server. Press enter.

Figure C.11: VMware Reboot

12. VMware ESXi 5 is now installed.

Figure C.12: VMWare ESXi Installed

13. To download and install vSphere client. Go to the URL https://192.168.43.128 on the Internet explorer. Download and install the client from the web.

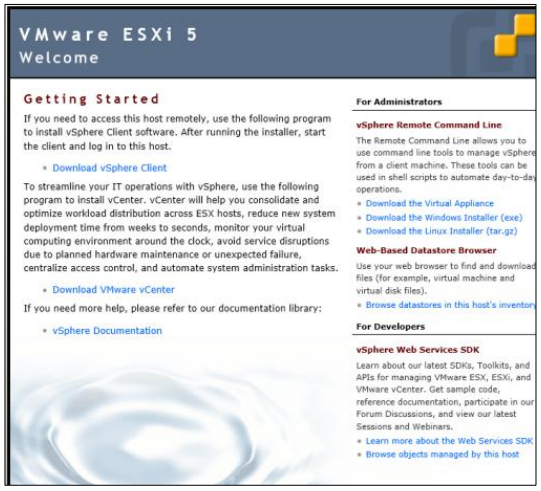

Figure C.13: IE with ESXi URL

14. To start vSphere client. Enter the IP address of vmware ESXi host, username and password.

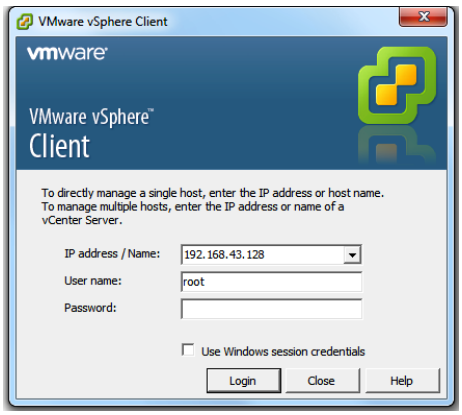

Figure C.14: vSphere Client

15. ESXi 5 is ready to host virtual machines.

Figure C.15: ESXi Management Console

Creating the Virtual Machines

16. Right click the server IP address and choose New Virtual Machine.

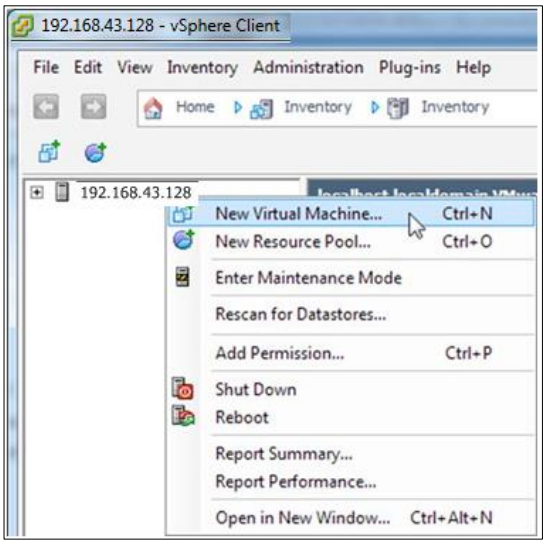

Figure C.16: New Virtual Machine

17. Assigning a unique name to the new virtual machine.

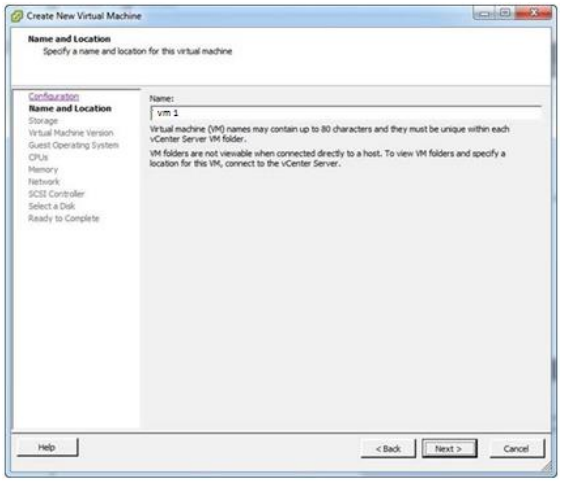

Figure C.17: VM Naming

18. Select the datastore to deploy the VM.

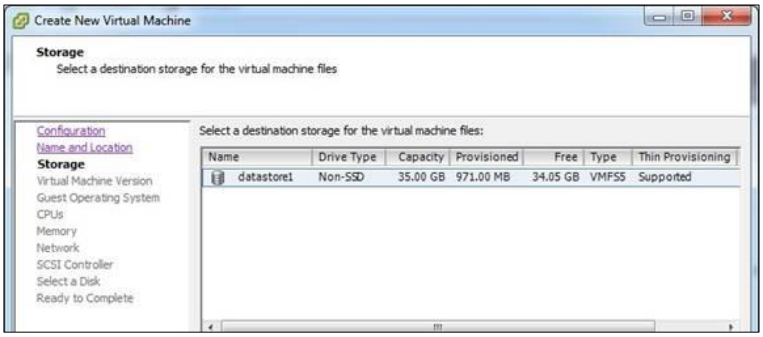

Figure C.18: Data-store to reside VM

19. Inside the virtual machine, the operating system will run. For the research work, backtrack 5r3 OS is installed as VM 1, so the Linux is selected.

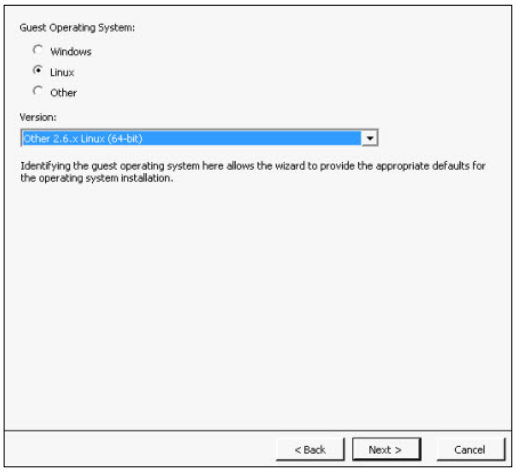

Figure C.19: OS for the Virtual Machine

20. Choose the number of NICs to add to the virtual machine.

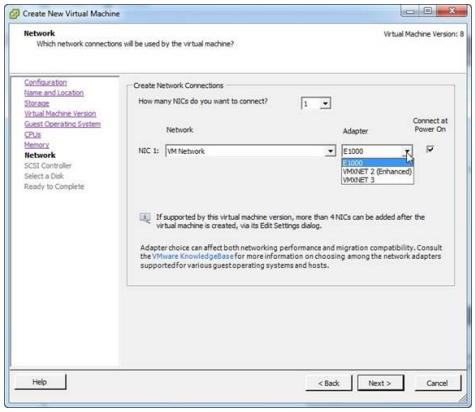

Figure C.20: Assigning NIC to the VM

21. Select the disk space for the virtual machine.

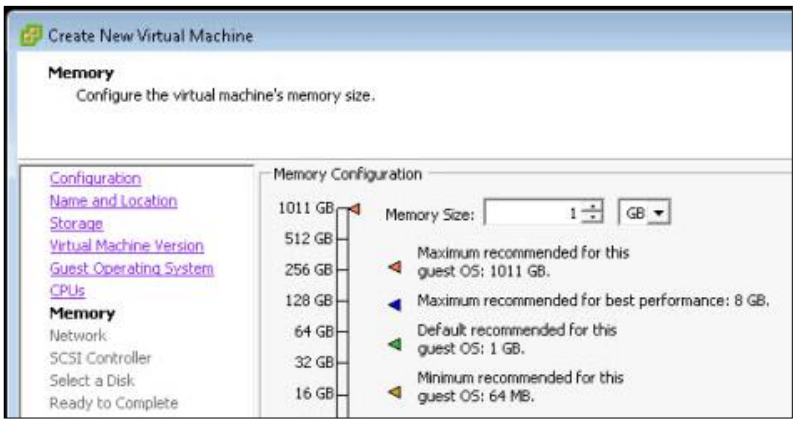

Figure C.21: Disk Space for VM

22. VM is installed.

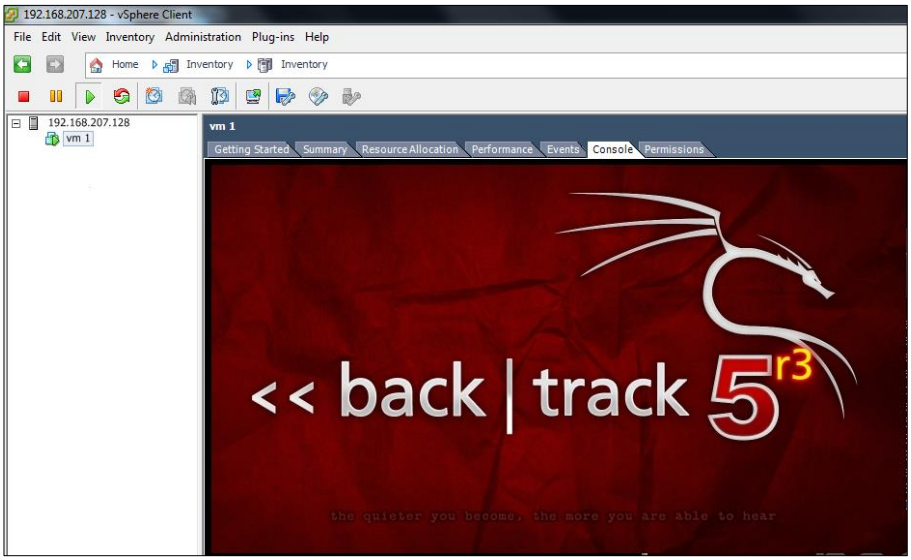

Figure C.22: Backtrack VM