FACHHOCHSCHULE KIEL
University of Applied Sciences

Fachhochschule Kiel

Faculty of Computer Science and Electrical Engineering

Master Project

AN ANALYSIS OF THE DOS ATTACK ON A CLOUD-BASED ENVIRONMENT

Submitted to

Prof. Dr. Christian Krauss

Fachhochschule Kiel

Faculty of Computer Science and Electrical Engineering

Date of Submission: October 23, 2018

ABSTRACT

Cloud computing is regarded as one of the most promising technologies in computing today. Flexibility and rapid elasticity have brought more convenient but with huge security risks and vulnerabilities according to which cloud services (SaaS, PaaS, IaaS) are intended to deploy. Cloud computing has introduced a new way of interacting with computing resources which comes with a variety of security risks and attack techniques into the cloud environment and DoS is among major risks. The attacker can fully or partially degrade the quality of the network or fully break down the victim's network connectivity. The main intention of a DoS attack is to make the victim unable to access or utilize the resources of a specific network. In most of the scenarios, targets could be internal or external network resources, storage, CPU, web servers etc. In a cloud environment also, a DoS attack can moderate the performance of cloud services significantly by damaging the virtual servers. The intention of this paper is to describe some scenarios of DoS attack and its effect which will show how vulnerable a cloud system can be and what are the consequences after a DoS attack.

TABLE OF CONTENTS

List of Figures

CHAPTER 01: GETTING STARTED

1.1 INTRODUCTION

It has been always a challenge for an organization to maintain these three issues: data storage, computational/ processing power and service availability. Due to the increasing percentage of device availability people own more than one device and always interact with the computer system. Moreover, most of the devices are connected to the internet and it has made easier to interact anytime, anywhere and by any means. According to Mark Weiser's 'three waves of computing' now we are in the era of the third wave of computing where many computers serve one (each) person. [1]

To fulfil these requirements it is very essential to have huge storage, strong computation power within a short span of time with maximum availability. That is how the cloud computing has been introduced. It has become the buzzword of today's modern technology. According to NIST definition: [2]

> *Cloud computing is a model for enabling 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 promotes availability and is composed of five essential characteristics (On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured Service); three service models (Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), Cloud Infrastructure as a Service (IaaS)); and, four deployment models (Private cloud, Community cloud, Public cloud, Hybrid cloud).*

The *on-demand self-service* refers to the provisioning capability of the users without human interaction.

The *broad network access* refers to the accessibility of the cloud services over the internet by various end user devices.

The *resource pooling* refers to the provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. [3]

Rapid elasticity refers to a user's ability to request or withdraw any additional space or services automatically without human interaction.

Measured service refers to a setup where cloud systems may control a user or tenant's use of resources by leveraging a metering capability somewhere in the system. [4]

There are three service models, Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS), which we will discuss briefly in chapter 03.

There are four deployment model of cloud computing, which are:

Private Cloud

The cloud infrastructure provided by a single organization among multiple consumes and owned, managed and operated by the organization.

Public Cloud

The cloud infrastructure is provided for open use by the general public and owned, managed and operated by an academic, business or government organization.

Community Cloud

The cloud infrastructure is provided exclusive use by a specific community and owned, managed and operated by one or more of the organization in the community.

Hybrid Cloud

The cloud infrastructure is a cloud computing environment that uses a mix of on-premises and utilizes both public and private clouds to perform distinct functions within the same organization.

1.2 RELATED WORKS

There are several numbers of research papers published and new techniques are being invented to perform attacks and defend attacks from the DoS vulnerabilities. DoS attack is a very serious security threat that can make a machine or a network resource unavailable to users. The main intention of a DoS attack is to make the network performance slow or make a website or service inaccessible.

Cloud computing provides dedicated, pay-per-use images of virtual machines which are accessible with less downtime or without downtime of an infrastructure. It is very cost effective for storage or powerful machine without compromising any performance of a system. Rapid elasticity has provided the ability to dynamically reallocate resources for filtering, encrypting, authenticating, traffic shaping etc.

The Internet of Things (IoT) is a novel paradigm that is rapidly gaining ground in the scenario of modern wireless telecommunications. [5] The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. [6]

In recent years, the Internet of Things (IoT) is being used widely in various domains. Much research has been focused on IoT nowadays. The research survey [7] reported that the number of connected device will grow to nearly 8 billion devices for the year 2020 excepting mobile phone, and home devices has the biggest portion of them about 3.7 billion. Which indicates these devices will generate a huge amount of big data (sensory data) and information and it will roam around the world wide web and perhaps the unauthorized entity will feel interested to look up or obtain (hack) the private data. It is true that, smart devices have made the daily life simple and it is easier to communicate with the home devices. With simple instruction, the devices connected to the network

interact automatically. With the help of smart home technology, it is easier to collect real-time data, for example, the room temperature, the amount of water in the house container. It is not only used in house but also in various wide areas around such as healthcare system, disaster management system, environmental monitoring, smart building etc. Though the devices are connected to the internet it is convenient to connect or communicate from a remote area. The connecting objects are enabling new functions, but it is also inviting some security threats besides. If the IoT system is attacked a great property loss will happen including residents and industries. IoT system is also not free from cyber-attacks like Denial of Service (DoS) attack, man-in-the-middle (MITM), eavesdropping etc. [8]

With a lot of advantages, it also includes some sort of drawbacks also. Security threats such as data breaches, data loss, system vulnerabilities, malicious insiders, Denial of Services etc. regarded as more harmful to a cloud network.

The goal of this paper is to highlight some of these attack techniques, analyze vulnerabilities around the cyber world and showing some path to mitigate the vulnerabilities among the cloud network.

CHAPTER 02: PROJECT GOAL AND REQUIREMENTS ANALYSIS

2.1 PROJECT GOAL

2.1.1 Analyzing cloud vulnerabilities

Before starting with cloud security, we have to analyze the threats and vulnerabilities regarding a cloud interface. Our first step would find out the common security threats and try on our local network or private cloud to determine the effect and take some initial countermeasures to resolve or mitigate the threat to secure local network or cloud network.

2.1.2 Applying cloud vulnerabilities

There are a wide range of DoS attack techniques such as Volume Based Attacks, Protocol Attacks, Application Layer Attacks. Among these three we would like to focus on volume-based attacks and protocol attacks. We will perform UDP flooding attack and ICPM ping attack which are known as volume-based attack and SYN flooding attack which is a part of protocol attack. To perform these attacks, we need some scenarios. Our initial plan and target is to perform the DoS attack in three different scenarios, such as:

1) Perform a DoS attack from one VM to another VM of same network.
2) Perform a DoS attack from one VM to another VM of different network.
3) Perform a DoS attack to Controller and try to make it unavailable for services.

To perform these experiments, we would require a private cloud to understand and analyze a real-time cloud environment.

2.1.3 Data collection

We would capture data using Wireshark by performing the different attack on our custom build platform. Then, we would customize the data to format it in ‘CSV’ so that we could process it further using EXCEL. In EXCEL, we would use a Pivot table and power pivot

to analyze our data and pivot chart to visualize our pivot analysis data. We have chosen 'Microsoft EXCEL' to find our desired insights and it is a very powerful data analytics tool. The pivot analysis provides very good and quick insights about data inconsistency and we can summarize a great deal of data efficiently and effectively.

2.2 WORKING PLATFORM: KALI LINUX

Before we start to write about why we have used 'Kali Linux' as our platform we would like to describe shortly about penetration testing.
If we define penetration testing, then:

> Penetration testing is a simulation of an attack to verify the security of a system or environment to be analyzed. This test can be performed through physical means utilizing hardware, or through social engineering. The objective of this test is to examine, under extreme circumstances, the behavior of systems, networks, or personnel devices, in order to identify their weaknesses and vulnerabilities. [11]

In simple, Penetration is to use some penetration testing tools or programmed app to attack a system or network (with permission) to analyze the weakness and find the vulnerabilities of that specific system. A penetration test can be performed manually or can be automated with software applications. Firstly, gathering the information related to that system, identifying possible entry points, (such as performing a network map), attempting security break and reporting back the findings.

There are many different tools which can be used for penetration testing. They are available in the marketplace and many of them are free to use. Some of them are even able to be customized which are known as open source tools and can be used to any platform such as Windows, Mac or Linux distribution. For this reason, Kali Linux is the best because it comes with the various tools for penetration testing and it contains a suite of penetration tools. Kali Linux is a Debian-derived Linux distribution and It is maintained and funded by Offensive Security Ltd. We did all of our experiment on Kali Linux

environment and as a host computer, we have used both Windows and Linux operating system.

2.3 ATTACKING TOOLS

There are literally many DoS and DDoS attacking free tools available, that can be used to perform and execute a DoS attack which can easily flood a server and can denial the victim network.

Within Kali, we can find many tools available on internet today and here we are figuring out some of them common and effective tools for kali Linux to perform a DoS attack.

2.3.1 LOIC

The LOIC is stands for Low Orbit Ion Canon and it is an open-source stress testing application. It is one of the most common tools for DoS attack which allows for both TCP and UDP protocol layer attacks. This tool is freely available on the Internet and available for windows and Linux. [80]

2.3.2 Pentmenu

Pentmenu is a bash script for recon and denial of service (DoS) attacks that is designed to be a simple way to implement various network penetration testing functions, including network attacks and commonly installed on most linux distributions. [81]

2.3.3 Xerosploit

Xerosploit is a penetration testing toolbox whose function is to perform the denial of service (DoS) attacks and man in the middle (MITM) attacks. It is a powerful tool for perform a DoS attack and can be used to perform Injection attacks. [82]

2.4 HARDWARE AND TOOLS

For cloud interface: ‘FH Kiel’ private cloud.

For local network: Our own local network consisting of our own computers.

Virtualization:	Virtual box installed on local computer and two operating systems to experiment vulnerabilities inside the virtual environment.
Visualization:	Excel and Pivot analysis tool.

2.5 REQUIREMENT ANALYSIS

To fulfil the project goal a list of requirements should be determined. Our project consists of three parts: First, analyze the security risks, second, implementing some attack techniques and collecting the data to understand the effects after deploying vulnerabilities, third, try to figure out some resolving/ mitigation techniques to secure the environment/ cloud interface from related vulnerabilities.

According to first step,

We would gather the information on security threats as well as for cloud computing to accomplish our analyzation part.

Secondly,

We would implement the attack techniques (described above) to measure the vulnerability inside the cloud network or local network and would collect the generated data for further analysis. For performing data analysis, we would use Wireshark to capture and then customized data to our desired format. We would use ‘EXCEL 2013’ for our pivot table and power pivot Analysis and we would use ‘Pivot Chart’ for visualizing the gathered data.

Finally,

We would try to find some mitigation techniques to resolve or mitigate the incoming vulnerabilities among the local network or cloud network.

CHAPTER 03: CYBER SECURITY AND VIRTUALIZAITON

3.1 CYBER SECURITY

Cyber security is an approach to protect cyber space from cyber-attack. Information security is all about protecting availability, confidentiality and integrity as this is a major asset for cyber security. As a definition of cyber-attack is:

> *A cyberattack is deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyberattacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft.* [12]

A cyberattack may include consequences such as, malware or trojan distribution, phishing, spamming, spoofing, identity theft, breach of access, denial-of-service and distributed denial-of-service attacks.

If we consider cyber-attacks, the cybercriminals often target less developed countries to exploit vulnerabilities. Due to the weak security and maintenance, it becomes easier to overload more and more traffic to the targeted system and make the network/ server/ computer to distribute or exploit their vulnerabilities. Furthermore, these computers work as botnets of the attacker and lately it helps to fulfil attacker's intention to gain access to big multinational companies. If one of the sectors compromised than the security of the entire system could be compromised which leads to a serious security breach. [13]

3.2 DATA BREACHES: SOME REASONS

In the cyber-world, data breaches are everyday phenomena. In a study conducted by Cisco in 2008, it was found that 33 percent of IT professionals are concerned that USB drives are the main causes of data leak. Meanwhile 25 percent say email is their top concern. Others are concerned about the negligent employees (39%), hackers (30%) and

disgruntled employees (20%). It was also reported that unauthorized use of applications has contributed to 25% of data loss incidents. The rate was seen bigger in India (79%) and in the US (74%). [14] There are some common reasons of data breaches which is happening frequently.

In an organization:
- Less or inadequate maintenance, not updating the security patch on a regular basis.
- Less control of admin privileges.
- Less monitoring and control of access to cyber systems.
- Poor or no policy and standard management in place.

Insider:
- Sharing the same file or same user group.
- Transferring file between home and work computer.
- Sharing the password with co-workers.

Hacker and malware:
- Day by day hackers are inventing new techniques to deploy their spam or malware.

- Botnets are really helpful to a hacker to implement Distributed Denial-of-Service and exploit severe vulnerabilities.

Cloud Computing:

- Anytime, anywhere, any device access has made a serious security issue in cloud computing.

- Some IT security professional has defined the 'Cloud' as a 'perfect storm' of data breach.

- The technical reason for calling this for three factors: mobility, cloud and virtualization.

3.3 RECENT DATA BREACHES

3.3.1 Singapore's historic data breach:

Singapore has suffered the most serious attack in the nation states history, impacting 1.5 million patients to SingHealth's specialist outpatient clinics between 1 May 2015 and 4 July 2018. [15]

- Attacked on 4th July, 2018
- Investigation confirmed that it was a cyber attack on 10th July.
- The personal information of 1.5 million patients was stolen, including name, NRIC number, address, gender, race and date of birth.
- Furthermore, 160,000 patients had details related to outpatient dispensed medicines stolen.
- Lee Hsien Loong, Singapore Prime Minister, had his personal particulars stolen and also the medicines record which was described as "specific and repeated" targeted attacks.

3.3.2 Data breach hits British Airways:

Financial data has been stolen from potentially hundreds of thousands of British Airways customers who made online bookings in recent weeks, extending a run of embarrassing technological mishaps suffered by the UK flag carrier. [16]

- The data breach occurred between 21st August and 5th September 2018, confirmed by the parent International Airline Group.
- Affected on bookings made on the airline's website.
- Around 380,000 card payments were "compromised".

The widespread of ordinary data breaches around the world demonstrate how real the danger is and the hackers are increasing their technical expertise to make the information systems as well as the cyber world more critical and vulnerable.

3.4 VIRTUALIZATION

Virtualization technology was developed in the late 1960s and allows to create multiple simulated environments to make more efficient use of hardware. [17] Virtualization dedicated and distributed the resources from physical hardware system. It uses an abstraction to make software to behave like hardware and it also adds corresponding benefits in terms of flexibility, reliability and overall performance. [18] It creates virtualization layer between the hardware components and the user. This enables the creation of virtual machine which are virtual computers that can run in multiple on a single set of hardware.

Virtualization involves in the use of encapsulating software such as Hypervisor or Virtual Machine (VM) underlying an operating system which provides the same behaviour that expected from a physical device. Virtualization takes physical resources such as memory, network interface and turns them into virtual resources for the virtual machine.

There are lots of benefits to virtualization: [18]

- Increases efficiency and multitasking because a user can run multiple computers instead of just a single computer running on computer hardware and can run multiple operating systems.
- It also increases manageability and increases security by isolating virtual machines from one another and isolating them from the core system as well as isolating applications and the ability to run legacy applications that wouldn't be possible sometimes on a regular company computer.

3.4.1 WORKING PRINCIPLE OF VIRTUALIZATION

Hypervisors separate the physical resources from the virtual environments and can place on top of an operating system or can be installed directly onto hardware which is virtualize. The hypervisors can take physical resources and separate, divide them to the virtual systems.

Physical resources that are separated from the physical environment as needed to the many virtual systems. Users interact and run computations within the virtual environment that is called virtual machine. The functions of virtual machine like any digital file, it can be moved or copied from one to another computer and it is expected to work the same.

When the virtual machine is running, and a program issues an instruction that sometimes needs some additional resources from the physical hardware, the hypervisor relays the request to the physical system and caches the changes.

3.4.2 ADVANTAGES AND DISADVANTAGES OF VIRTUALIZATION

Virtualization has many benefits over it is hardware resource utilization, energy saving, costs and makes it possible to allow to run multiple applications and various operating systems on the same server at the same time. Virtualization manage and control the resources effectively.

- IT operations increase and provides easier backup and disaster recovery.
- It maximizes the server capabilities, reducing maintenance and operation costs
- A user can run multiple platforms on a single server.

Compared to the multiple advantages that it offers, drawbacks of virtualization are almost negligible.

- It has a high cost of implementation.
- It creates scalability and availability issues.
- Sometimes IT staff are not aware of virtualization, therefore they need to be trained.

3.4.3 TYPES OF VIRTUALIZATION

Virtualization are divided into many forms depending on the type of application use and hardware utilization. [19]

1. **Hardware Virtualization:** This is the most common type of virtualization and known as server virtualization or hardware assisted virtualization. This type of virtualization is made by a virtual machine manager that called “hypervisor” and the resource allotment is done by the hypervisor. The main advantage of Hardware virtualization is because of maximized hardware utilization and application uptime. It allows a user to run different operating systems at the same time on the same machine.

2. **Software Virtualization:** Software Virtualization creates the function of multiple virtual environments on the host machine. It is an isolating strategic virtual machine and used for virus testing, for an example honeypot for attackers. It creates a complete computer system that run the guest operating system with higher efficiency in resource utilization.

3. **Desktop Virtualization:** This is one of the most common form of virtualization that separates the desktop environment from the physical device and enables to store a user´s desktop on a remote server. The major advantages of this type of virtualization is that the user can access his/her desktop from any location, from any device and users are able to access their personal files, documents and applications.

4. **Network Virtualization:** Network virtualization is a method where multiple sub networks can be created on the same physical network that combines all physical networking equipment into a single resource. It divides the bandwidth into multiple, independent channels and assigned each of to real time devices. It increases reliability and allows better monitoring and identification of data usage.

5. **Storage Virtualization:** Storage virtualization is very easy and cost-effective to implement where multiple physical storage devices are grouped together. It compiles user's physical memory into a single cluster. The main advantages of this type of virtualization is that providing of homogenization of storage across multiple capacity of storage devices. It can reduce the downtime and load balancing for better optimization of performance.

3.5 HYPERVISOR

The hypervisor is the key to enabling virtualization, it´s software installed on top of computer hardware. It creates the virtualization layer and acting as a platform for the virtual machines to be created on. A hypervisor is a program or a process that for create and run virtual machines and separate a computer's operating system and applications from the underlying physical hardware. [20] In simple words A hypervisor is a program that host several different virtual machines on a single physical computer.

The two main types of hypervisors are: [20]

- Type 1 Bare metal or native hypervisors: In this type the hypervisor also has it own operating system and can be installed directly on computer hardware. It creates the virtualization layer on top of which the virtual machines are created on. VMware type 1 hypervisor is the ESXI server.

- Type 2 Embedded or hosted hypervisors: In this type the hypervisor is a software application that installed on top of host operating system. It creates the virtualization layer in which a user can create a virtual machine. VMware type 2 hypervisor is VMware workstation professional, VMware workstation player and VMware fusion for the Apple operating system.

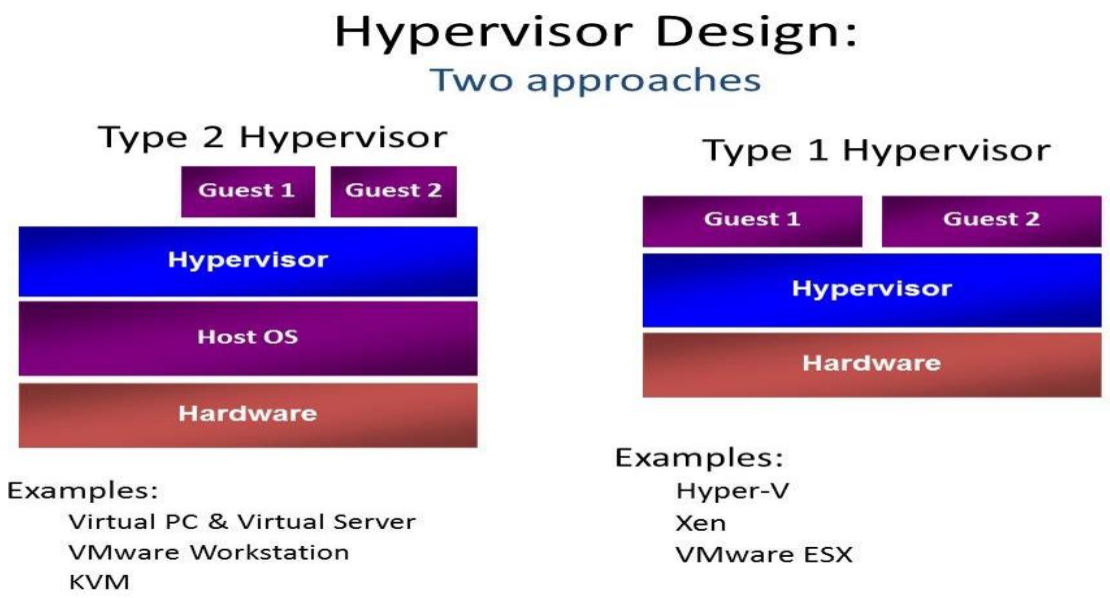


Figure 01: Types of Hypervisor [79]

3.6 VIRTUAL MACHINE

The basic idea behind the VM is it allows to run more operating systems or other operating systems within current (host) OS. Operating systems are called software able to control hardware because of their unique ability of controlling the hardware that they are put into their own special category of software. So, operating system which control the physical components of a computer namely the hardware. A virtual machine manager also called a hypervisor is another type of software that allows us to run more operating systems within an existing one for an example VirtualBox, VMware. Virtual machine or virtual computer needs all the same components that a regular component does. It needs storage, it needs access to a keyboard, it needs network interface cards, it needs processing and it needs RAM. Virtual machines can easily move and can be easily copied to optimize hardware resource utilization between host servers.

The VMs use many of important management considerations where many of which can be addressed through general systems administration along with the best practices and

tools. In consolidation there are some risks that includes some overtaxing resources on multiple virtual machine. [21] It is possible to share the same hardware platform for hundreds of virtual machines. But it does add some risks, if the hardware platform fails, it could take out your hundreds of virtual machines.

3.7 VIRTUALIZATION VS CLOUD COMPUTING

Virtualization technology that creates some dedicated resources or can create multiple simulated environments from a single and physical hardware system where hypervisor directly connects to that hardware system and allows to split one system into separate and distinct environments known as virtual machines (VMs).

Cloud computing is a methodology and known as a set of principles and also a set of approaches which can deliver the storage infrastructure resources, services and network platforms, and can pool an automate virtual resources for on-demand use. It delivers variable resources to groups of users for a variety of purposes.

Virtualization differs from cloud computing, because we can say easily that virtualization is a software that manipulates the hardware, and on the other side cloud computing refers to a service that results from that manipulation.

CHAPTER 04: CLOUD COMPUTING

4.1 DATA SECURITY

This section is focusing on some main aspects when we consider the IT security and attacks. Based on the TCP/IP protocol suite this includes a broad classification for the attacks, against which the attacks presented.

The concepts about the Data and IT security are divided into three different parts in short CIA triad:

Confidentiality, Integrity and Availability. [22]

Confidentiality

Ensures that only by an authorized person are allowing to access the sensitive information and kept the data or information away from those who are not authorized to possess them. Security measures can then be implemented accordingly using security mechanisms such as usernames, passwords, access control lists, and encryption.

Integrity

Ensures that the format of the information is true and correct and it's in original purposes or simply Integrity is relating to the trust that we have about data. The authorized persons can only edit the information and remain in its original state. Integrity can be implemented by using the security mechanisms such as data encryption and hashing.

Availability

Ensures that the availability of information and resources where those are of course important in running a business. It can be implemented by using some security methods such as network optimization, hardware maintenance and software patching. To guard against downtime and unreachable data dedicated hardware devices can be used.

4.2 CLOUD COMPUTING

Cloud-based computing has introduced an attractive solution among the organizations which are operated across the world or some of the organization who need computing power or resources for short span of time. It is cost saving and it has rapid elasticity. Centralized data centres or dedicated servers are set up to host cloud services. Moreover, it also brings privacy and security and data remains safe among to the consumers. To ensure cloud security various security standards have been proposed or being developed by standard bodies like Cloud Security Alliance (CSA), International Organization for Standards (ISO), National Institute for Standards and Technology (NIST) etc. To control the security and privacy most cloud providers are implementing a mish-mash of security and privacy controls.

Although we have so many security standards, unfortunately, the cloud is not entirely secure from various vulnerabilities or cyber-attacks. Before we deep down to the cloud attacks we would like to highlight which services are provided by cloud computing. There are three service models offered by cloud computing, which are:

- ✓ **Software as a Service (SaaS)**
- ✓ **Platform as a Service (PaaS)**
- ✓ **Infrastructure as a Service (IaaS)**

We will discuss about these three service models gradually.

4.3 CLOUD MIGRATION

Cloud Computing is a major trend that will have a significant impact on the IT industry. Could Computing is suitable for building flexible and scalable systems. [23] Migration into the cloud is not so easy to accomplish. The main problem of migration is that the applications of the organizations are not designed to perform at cloud interface. The first obstacle is to redesign and adapt those existing applications to a new cloud environment. The migration barrier can be related to this: [23]

- Big budget problem.
- Workload of designing, coding and testing.
- Lead time for software delivery.
- Difficulty to make mash-up application.
- The migration workload is huge.
- HTML templates runtime
    - Graphical User Interface (GUI) recognition.
    - HTML templates are semi-automatically generated.

After a huge drawback cloud migration is not impossible. A real-world data migration example is given below.

4.3.1 REAL-WORLD CLOUD MIGRATION

New York Times wanted to create a digital historic news library for 1851 – 1922. [24]
To make the data digital the organization had to deal with a series of large TIFF images, associated metadata and article text captured from OCR. This all adds up to terabytes of data and it was not easy to deal with. Fortunately, the found the Amazon web services and they were able to do it with less effort.

Challenges: [24]

Using Amazon Web Services, converting

405,000 very large TIFF images,
3.3 million articles in SGML
405,000 xml files

Into,

More web-friendly 810,000 PNG images (thumbnails and full images)
405,000 Javascript files.

Solution: [3]

Utilized hundreds of virtual machines concurrently running on Amazon EC2 the migration was done in less than 36 hours.


The New York Times.

ROOSEVELT FREEZES WAGES, RENTS, FARM PRICES; NAMES JUSTICE BYRNES ECONOMIC DIRECTOR; U. S. TROOPS MOVE OUT TO A NEW ALEUTIAN BASE

Figure 02: Picture from New York Time old archive.[25]

4.4 SOME TERMINOLOGIES ABOUT CLOUD COMPUTING

4.4.1 INFRASTRUCTURE AS A SERVICE (IaaS)

Infrastructure as a service (IaaS) is a form of cloud computing that provides virtualized computing resources over the internet. [26]

In an IaaS model:

- A cloud provider mainly hosts the infrastructure components and its traditional presence in an On-Premises data centre. Including Servers storage, Networking Hardware as well as the Virtualization and Hypervisor layer. [26]

- Gives users the facility to collaborate between the services and different elements of this model. [26]

According to NIST definition: [27]

> *The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).*

IaaS cloud models is a complex multi-layered system and this infrastructure has a complex structure. As an end-user, the service quality and reliability depend on the underlying software/ hardware infrastructure, the used technologies and resources. IaaS is an effective model for temporary or experimental workloads, which can change unexpectedly.

IaaS Examples:

Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE), Joyent

4.4.2 PLATFROM AS A SERVICE (PaaS)

Platform as a Service (PaaS) model provides a complete development and deployment environment in the cloud. Like IaaS, it includes the hardware - storage, servers, networking- but also the middleware, development tools and applications. The PaaS model provides a framework that developers can build, develop or customize cloud-based applications.

According to NIST definition: [27]

> *The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.*

In an PaaS model:

- Provides the facility to install and utilize both software/ application and hardware.
- Provides a platform for the users to establish their own environments.
- PaaS includes the development tools with pre-coded application components.

PaaS Examples:

AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos, OpenShift.

4.4.3 SOFTWARE AS A SERVICE (SaaS)

Software as a Service (SaaS) is a multi-tenant software architecture to provide flexible customization to the individual tenant. SaaS platform is a very different platform than traditional software architecture. It provides unique user experiences among the consumers/ users with high performance in a multi-tenant environment concurrently.

According to NIST definition: [27]

> *The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.*

SaaS software architecture should solve the problems that the traditional software does not have faced, such as: [28]

- Mass data storage and access.
- Unpredictable security threats from the internet.
- A variety of individual needs
- Customized and convenient user experience
- Reliable trust from users.
- How service provides sustain operations and maintenance management.
- Open API for integration.

SaaS Examples:

Google Apps, Dropbox, Salesforce, Cisco WebEx, Concur, GoToMeeting.

4.4.4 EVERYTHING AS A SERVICE (XaaS)

Although there is no NIST definition of 'XaaS' but it persists in the real world. Everything-as-a-Service (XaaS) is a cloud computing term for the extensive variety of services and applications emerging for users to access on demand over the Internet as opposed to being utilized via on-premises means. [29]

Some examples are given below:

Storage as a Service

- Providing data storage or file storage.

Security as a Service (SECaaS)

- Providing services for improving data security, such as data encryption, authenticity and access control, integrity validation etc.

Disaster Recovery as a Service (DRaaS)

- Keep track of system changes, provide full system restore as a service in case of disaster or damage.

Identity as a Service (IDaaS)

- Provide login services, access control management, single sign-on as a service.

Business Process as a Service (BPaaS)

- Provide full business process modelling, management and execution runtime as a service

Logging as a Service (LaaS)

- Provide log data storage, analysis and management as a service.

4.4.5 CLOUD MODELS: A COMPARISON

The organizations select their cloud models according to their requirement and the service they provide. Every cloud model has some advantages and disadvantages and unique user/ consumer interface or maintenance capability. The cloud service models (Iaas, Paas, SaaS) provides different architecture models to enhance the user experience. The table gives a short explanation of the service provided by three different cloud service models.

	On-Premises		IaaS		PaaS		SaaS
Cloud User Manage	Application	User Manage	Application	User Manage	Application	Provider Manage	Application
	Data		Data		Data		Data
	Runtime		Runtime	Provider Manage	Runtime		Runtime
	Middleware		Middleware		Middleware		Middleware
	Operating System		Operating System		Operating System		Operating System
	Hypervisor	Provider Manage	Hypervisor		Hypervisor		Hypervisor
	Servers		Servers		Servers		Servers
	Storage		Storage		Storage		Storage
	Networking		Networking		Networking		Networking

Table 01: Comparison between three cloud service models.

CHAPTER 05: CLOUD VULNARABILIITES

5.1 TCP/IP PROTOCOL

To understand the security threads and to perform an attack one should have some basic knowledge about the concepts of how these protocols are intended to function. TCP/IP is the Transmission Control Protocol/Internet Protocol, is one of several network protocols and is a suite of communication protocols used to interconnect network devices on the internet developed by the United States Department of Defence (DoD) at the end of the 1970s. [30] It can also be used as a communications protocol in a private network and the reason behind designing such a protocol was the need to build a network of computers being able to connect to other networks.

TCP/IP provides end-to-end communications and specifies how data is exchanged over the internet, and can identify the packets, transmitted addressed, routing protocol and receiving the destination.

The two main protocols in the internet protocol suite serves specific functions. TCP- defines how applications can create channels of communication across a network and provides reliable, ordered delivery of data between applications running on hosts on a TCP/IP network. It's a connection-oriented protocol, before data sending, a connection between two hosts must be established and the process used to establish a TCP connection is known as the three-way handshake. TCP is used by applications that require high reliability such as HTTP, FTP, SMTP, SSH etc.

IP defines how to travel a data or a packet from source to destination address or simply routing each packet to make sure it reaches the right destination.

A TCP/IP communication through a network typically uses several packets where each of the packets have a sending address and a receiving address, including data and some additional control information. TCP/IP is not controlled by any single company, and the

internet protocol suite can be modified easily. The advantages of TCP/IP protocol suite, it is compatible with all operating systems, also compatible with all types of computer hardware and networks and can communicate with any other system.

5.2 DENIAL OF SERVICE ATTACKS

DoS attacks are common security threads to the part of every Internet user's life and they are happening all the time. A denial-of-service attack (DoS) is a security event where the attackers take an attempt, and that occurs when an attacker takes action to prevents legitimate users from accessing targeted a network resource. [31] DoS attacks are typically a type of attacks of servers flooding and networks with some unusual extra traffic in order to make the victim's resources unavailable and make it difficult for the users to use them. The attacker usually sends excessive messages to authenticate requests which may have invalid return addresses.

In a DoS attack the network will be unable to find the return address of the attacker and causing the server or network to in a waiting period whenever the connection trying to close. The attacker is ready to sends more authentication messages which have invalid return address before the server closes the connection. Hence, the attacker can keep the network or server busy with the process of authentication. DoS attacks do not have anything to do with your physical hardware, it doesn't take any control over remote hosts.

The attacker can perform a DoS attack in a several ways:

- Attacker can flood the network traffic to prevent or make it difficult for the legitimate users.
- To preventing access to a system or a service DoS attack can disrupt the connections between the two machines.
- To make a particular website unreachable or prevent to accessing any website.
- To send higher volume of spam email than usual.
- To down the whole local network for the legitimate users.

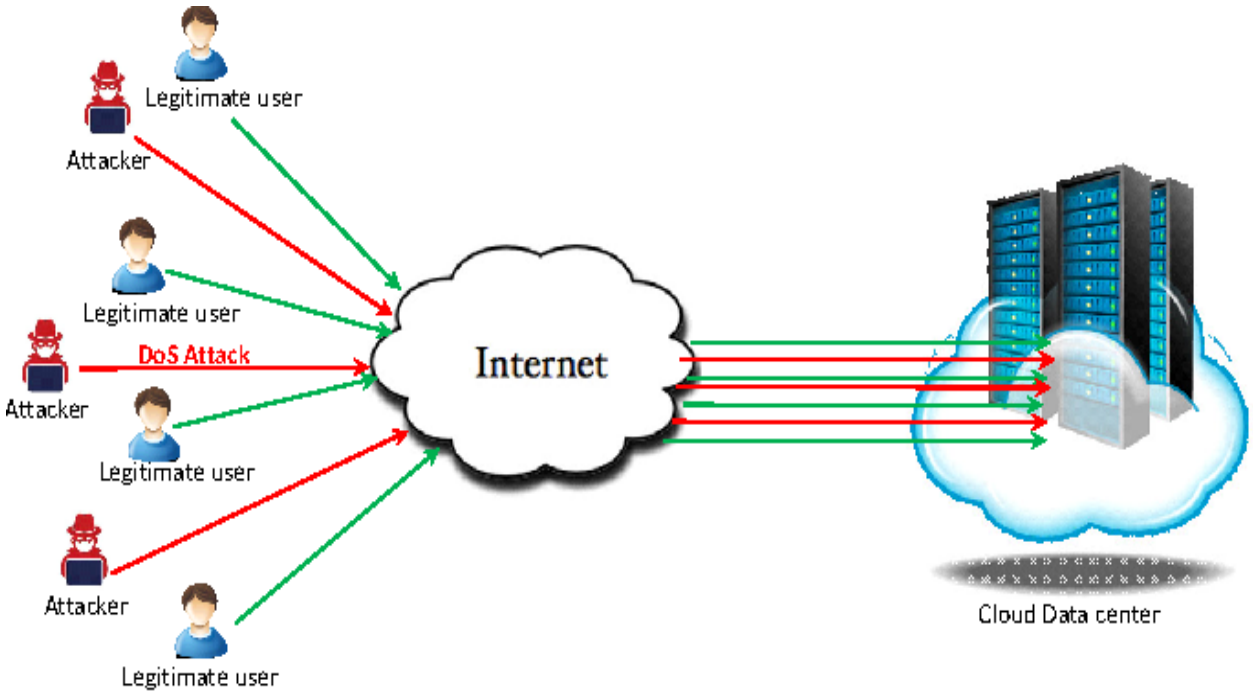


Figure 03: Description of the DoS architecture [44]

These types of DoS attacks are carrying very serious issue in our daily internet life and can cause a huge damage to the website or the network. Let's think about a bank website, a DOS attack can make a bank's website inaccessible and could lead to temporarily suspension of the website. However, a single attack or a single computer cannot DoS a website which has some website firewall safeguards, but only very small websites may be vulnerable to this. Hence, for taking down a good website attacker requires very large number of computers (DDoS) for attacking the server, network or website at the same time.

Sometimes Denial of Service attack can cause the following problems:

- Inaccessible services
- Interruption of network traffic
- Connection interference
- Ineffective services

5.2.1 DOS ATTACKS TODAY

It was an attack in early 2000 when Michael Calce, a Canadian high school student, managed to shut down one of the leading web powerhouses with a distributed denial of service attack. Over the years followed that, Michael successfully disrupted, other such sites as Amazon, CNN and eBay [23].

Since then, denial of service attacks has become a popular thread such the attacks are commonly used to a means of online activism, and even to wage cyberwar.

Over the years, the denial of service attacks has also gotten bigger attacking choice among the attackers. It would have been enough in the mid of 1990s, to bring down many systems with 150 requests per second where today the attacks can exceed 1,000 Gbps [23].

In terms of technology and attack scale, 2016 was the year of distributed denial of service attacks with major disruptions with 29,000 unique IP addresses around the world [25]. In Q4 2016, the geography of denial of service attacks expanded to 80 countries [26]. In 2016 China accounting for 76.97% where the united states stand for 7.3% and South Korea 7%. According to Q4 2016 report the SYN distributed denial of service attack was the most popular and accounted for 75.3% of attacks [25].

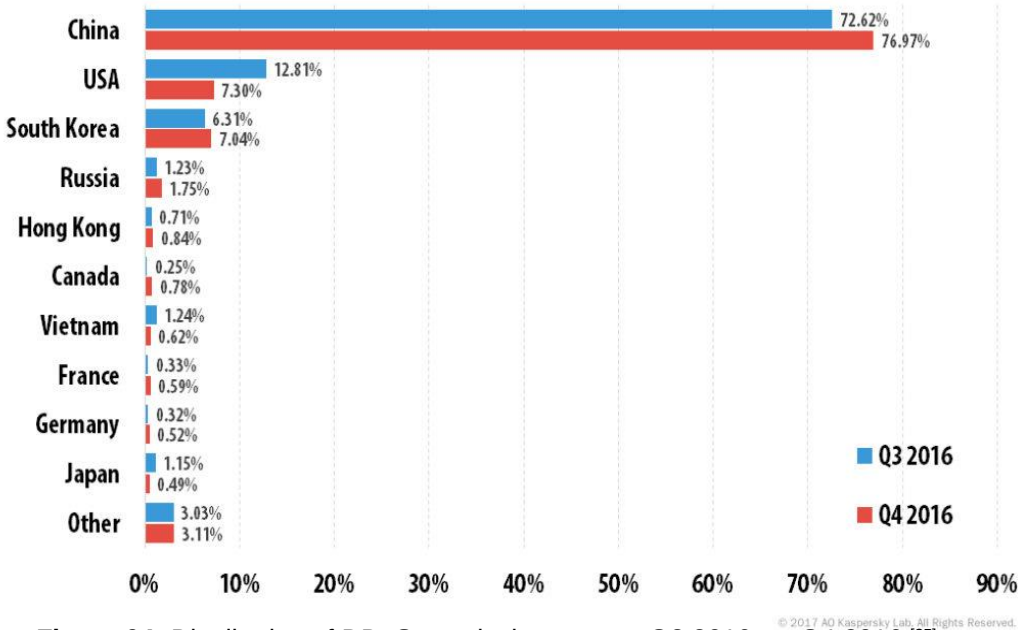


Figure 04: Distribution of DDoS attacks by country, Q3 2016 vs. Q4 2016 [35]

Q4 Summary

- In Q4 2016 80 countries were targeted by DDoS attacks where 71.6% of targeted resources were in China.
- In terms of the number of targets and number of detected South Korea, China and the US remained in the top.
- SYN DDoS, TCP DDoS and HTTP DDoS remain the most common DDoS attack scenarios.

5.2.2 CATEGORIES OF DOS ATTACKS

- **Volume Based:** It is the most common type of DoS attacks that an attacker like to perform. In volume-based attack the attacker can send a large volume of network packets or traffic to the target in order to inundate the network bandwidth. The high-volume traffic can choke the bandwidth of the network and can denial to other packets. Volume-based attack can be characterized by an immense amount of traffic. Attacker insert reflection medium and used a small amount of request and generate a huge number of network traffic. In reflection-based volume attacks, attacker uses a spoofed source IP address and can target a service by sending the legitimate traffic to a DNS server. [36] In such volume-based attack, the spoofed IP address is considered as the target of the attack where the goal is to surcharge the bandwidth of the spoofed IP address or the attacked site.

- **Protocol Based:** In Protocol-based attack the attacker aiming on exploiting weakness, server resources in the layer of 3 or layer of 4 in the OSI model and also targets the resources apart from bandwidth. In such case of scenario, the attacker targets the firewalls, servers, and other network equipment etc. TCP SYN flood attack is the most common type of protocol-based denial of service attack. Some other protocol-based attacks are fragmented packet attacks, ping of death attacks and more where ping of death attacks is popularly used to denial a victim's Bluetooth service. [36]

- **Application Layer:** It is the trickiest DoS attack and focus on web application. These attacks are considered as the most sophisticated type of attacks and which sends requests and network traffic to the server that are intended to overflow it. By sending a huge amount of request the attackers can crash the application server or can block the resources of the server. Attackers send some extremely slow, incomplete requests and keep the server in a waiting stage complete request. Hence, these attacks are most serious types of attacks as they are very effective and can generate low rate network traffic. In application-layer attacks request, traffic is usually legitimate and are comparatively harder to mitigate. [36]

5.2.3 TYPES OF DOS ATTACK

In this section we will discuss some common types of denial of service attacks which are available on the internet. These attacks always use the weaknesses of the TCP/IP protocol [37] and utilize the weaknesses in targeting TCP/IP protocol suite itself.

The most common types of DoS attacks are:

- **SYN Flood Attack:** A SYN flood denial of service attack exploits a common and known vulnerability in three-way handshaking or in the TCP connection sequence. The client takes an attempt and try to establish a TCP connection which is known as three-way handshaking to a system or a server. The both systems exchange a sequence of requests and this technique applies to all TCP connections. The client sends a SYN request, asking the server to open a TCP connection. After receiving the client's request, the server must be answered by a SYN-ACK response and then the client send a confirmation of ACK response. After established the connection, data can be exchanged between the client and the server.

  In a SYN flood scenario, the potential vulnerability arises when the server system sends an SYN-ACK back to client, but the client does not receive the ACK message or the client sends the multiple SYN requests from a spoofed IP address. On the other way, the host or the client continuously wait for the acknowledgement

(ACK message) for each of the requests, till then no new connections can be possible, hence resulting denial of service. When the victim server system receives the packet from the spoofed IP address or the attacker, it is difficult to determine its true source. The use of input source filtering can validate the source of a request as the network forward the packets based on destination address. [38]

Generally, in such type of scenario there is a timeout associated with a pending connection and then the victim's server system will recover. But the attacker can simply continue sending IP-spoofed network requests or packets asking for new connections faster than the victim system can timeout the pending connections. Increasing size of connections table can sometimes prevent the SYN flood attack. Some more possible defences are adding more servers and trace attack back to source. One of the major drawbacks of SYN flood attack is that, the hacker uses spoofed Ip Address, so that the firewall cannot completely block the SYN flood attack. [38]

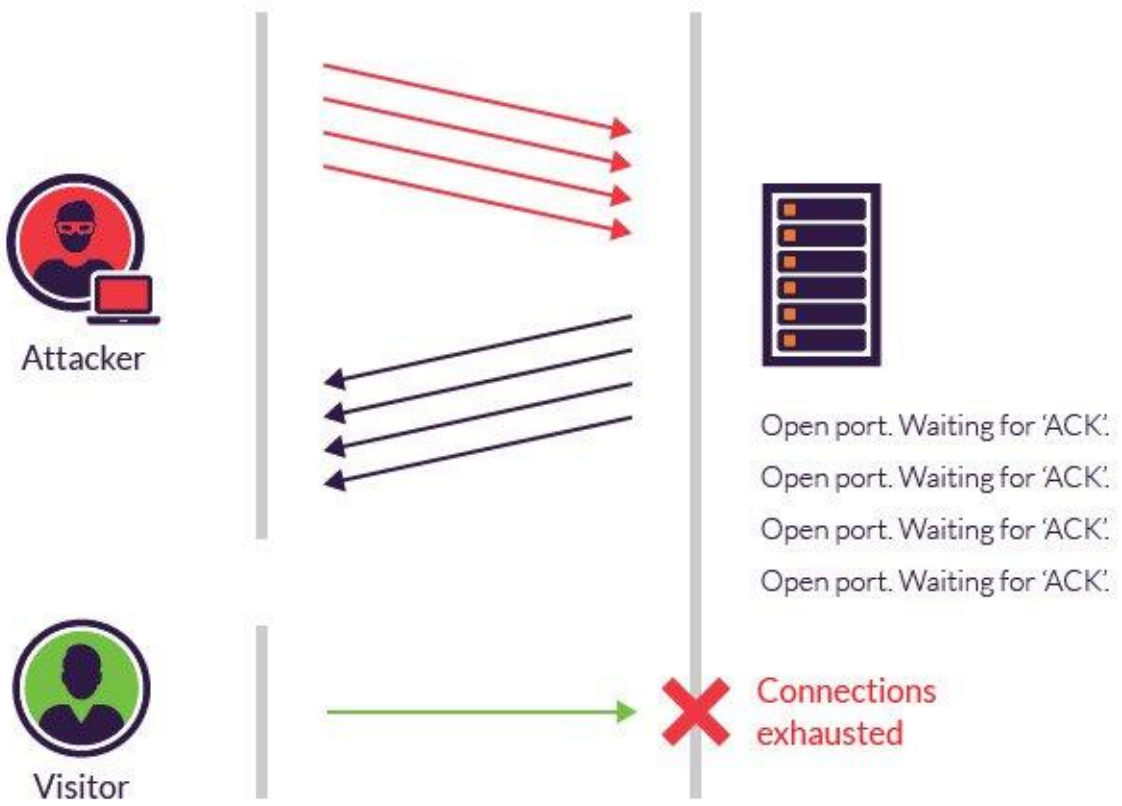


Figure 05: Progression of a SYN flood [39]

Some possible countermeasures for SYN flood attacks are:

1. Check periodically incomplete requests and randomly clear the incomplete connections. This can reduce the possibility of successful SYN attack.
2. Avoid allocating large memory for first packet, it is considered one of the best countermeasures.
3. Using of proxy server can be also reduce the SYN attack.
4. Circuit level firewalls can monitor the handshake of each new connection.
5. Increasing size of connections table can sometimes prevent the SYN flood attack.

- **UDP Flood:** A User Datagram Protocol is any denial of service attack where the attacker sends a lot of UDP packets. The attacker sends user datagram protocol packets to the random ports of a target in order to floods the target with UDP

packets. [40] These types of UDP flooding attack also belongs to a class of brute force attacks. When the victim receives the UDP packets then the victim system determine which application is waiting on the destination port.

The victim server system realizes there is no waiting application on the ports and then generate an ICMP packet of destination that is unreachable to the imitated source address. When a large amount of UDP packets forwards to the victim ports, the system may will go down which can ultimately lead to inaccessibility. Anyone who is connected in a network can be possible to cause a denial of service. Blocking unused all UDP services can reduce the possibility of UDP flood attacks.

- **ICMP Ping Flood:** ICMP ping flood attack is similar in principle to the UDP flood attack that broadcasting a bunch of ICMP packets. ICMP ping flood attack can overcast the victim resource with ICMP ping request or echo request. The attacker sends the echo request packets as fast as possible without waiting for replies. These types of attacks can consume and block both the incoming and outgoing bandwidth. The concept behind the ICMP flood attack is to send so much data and ping request to the victim server system that can make the system to slow down. Normally, the ping flood attacks surcharge a network by sending a continuous ICMP echo requests over a high-bandwidth connection. [40]

- **Ping of Death:** In a ping of death attack the attacker sends multiple malicious pings to the victim system. It is a typically a TCP/IP implementation attack. The target system or the victim receives an IP packet that is larger than the size which is allowed by the IP protocol. The maximum length of an IP packet is 65,535 bytes where the attacker sends an IP packet that exceeds the maximum of 65,536-bytes size. However, when the large number of packets arrives in target system and crashes the systems that are using a vulnerable TCP/IP stack. [41] In such types of attack scenario, the attacker sends an ICMP echo request to the victim system and the request is much larger than the maximum size of IP packet. When the ICMP

echo request received by the victim that is bigger than the normal IP packet size, as a result the OS may be crashed, rebooted and can say its performance will be affected.

- **Smurf Attack:** A Smurf attack is a type of denial of service attack in which the attacker sends an Internet Control Message Protocol (ICMP) ping message from a spoofed IP address that is flooded the targeted or victim server. These types of attacks can create high network traffic on the victim network. The attacker can send a huge amount of ICMP echo reply packets to a victim, which rapidly and effectively refusing its uses and services to the legitimate users and causing a temporary suspension of network. [41] The network administrators use ICMP to exchange information about the network state and use the echo request to determine their operational status. In this attack the attacker sends a spoofed network packet that includes an ICMP ping and can make the network unusable for real network traffic.

  The following steps can lead to a smurf attack:

  1. Smurf attack constructs a spoofed packet including its source address and set it to real IP address of the victim.
  2. A large amount of ICMP echo requests sends to the victim.
  3. The victim receives the requests and then responds to the spoofed address.
  4. It can build large amount of traffic on the side of victim's network and resulting in wreck of bandwidth which can crash the victim's server.

  A smurf attack can be avoided by disabling IP broadcasting addresses at each network and firewall. [42] The routers can be configured in a way to ensure that the packets are not forwarded which is directed to broadcast addresses.

- **TCP Flood Attack:** There are some other TCP flooding attack (TCP ACK flood, NULL flood, RST Attack) except SYN attack where it doesn't take any advantage of the TCP three-way handshake. But these types of attack can take advantage of other TCP's finite state.

In TCP flood attack, attacker sends lots of TCP ACK network requests or packets to victim and try to utilize the victim network resources. When the packets arrive in the victim ports, the ports might reply a TCP RESET packet that causes more traffics victim's network. Depending on the OS, it can be an open port or can be a closed port. [42]

In an RST attack the TCP Reset flag is used to abort TCP the connections. The host deletes the connection when the victim receives such a packet. The packets can be sniffed from the network. The attacker sends RST packets with with a spoofed IP address in order to turn down the active TCP connection effectively. The purpose and the effect of this RST attack is similar to SYN flood attack, but the attacker doesn't need to send large volumes of network traffics.

- **Slowloris Attack:** Slowloris attack operates at layer 7 of OSI model and is a highly targeted attack. These types of denial of service attack enabling one web server to take down another server with minimal bandwidth. Slowloris makes partial http connections to the host without affecting other services of the victim network. The attacker sends constantly more HTTP headers. The victim server opens the false connections and floods the connection pool. As a result, it leads denial of service.

  In a slowloris attack http session is active continuously for a long time and exploits a design approach of many web servers. Apache servers, dhttpd and Goahead web servers are affected by slowloris attack. In 2009 during the protests related to the elections slowloris attack was used against Iranian government servers. [43]

5.3 ACCOUNT HIJACKING IN CLOUD

In this sort of security threat, hackers look to capture the record by taking the security accreditation and afterward spying on the exercises and exchanges of clients. The hackers can likewise control the information, embedded false data and divert the customers to ill-conceived websites. This kind of weakness is especially terrifying because hackers can utilize the notoriety and the trust clients have developed to control the customers. In 2010, Amazon confronted an attack [45] [46] that enabled hackers to take the session ID's that give clients access to their records after entering their passwords. This left the customer's certifications presented to the hackers. The bug was traced and deleted 12 hours after it was found, yet numerous Amazon clients unconsciously fell for the assault amid that time.

5.3.1 Ways of hijacking:

In account hijacking, the hacker utilizes a fake email record to imitate the valid email account of original owner. Usually, account hijacking is devised through email phishing [47][48], sending satirize messages to the client, secret key speculating or a few other hacking strategies. By and large, an email account is connected to a client's different online administrations, such related systems and money related records. The hacker can utilize the record to recover the individual's close to home data, perform monetary exchanges, make new records, and approach the record proprietor's contacts for cash or help with an ill-conceived movement. Cloud account commandeering is a typical strategy in wholesale fraud plans. The assailant utilizes the stolen account data to direct malignant or unapproved action. At the point when cloud account capturing happens, an assailant commonly utilizes a traded off email account or different qualifications to mimic the record proprietor.

5.3.2 Business Perspective of Account Hijacking:

Cloud account hijacking at the venture level can be especially destroying, contingent upon what the attacker does with the data. Organization respectability and notorieties can be crushed, and private information can be spilled or distorted making huge cost organizations or their clients. Lawful ramifications are additionally feasible for organizations and associations in profoundly controlled enterprises, for example, medicinal services, if customers' or patients' secret information is uncovered amid cloud account hijacking occurrences.

5.4 IDENTITY AND ACCESS MANAGEMENT

Identity and Access Management (IAM) is about the administration of access of identities to information. As indicated by Jøsang and Pope: "A character is a portrayal of an element in a particular application area." [49] Identities are connected to an arrangement of qualities that characterize them inside the application area. Models of attributes, additionally called identifiers, are name, date of birth or record id. [50] A substance can have one or various characters inside an application space and every identity can have different identifiers and must have somewhere around one exceptional identifier inside the application area[49]. This unique identifier enables an identity to be perceived.

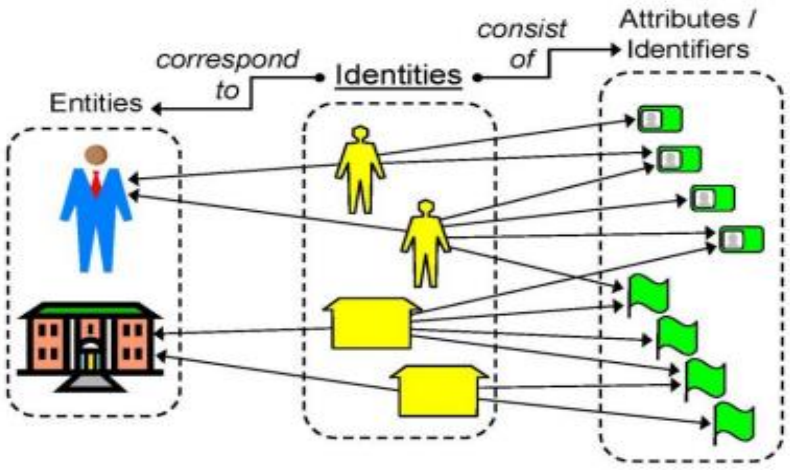


Figure 06: Correspondence between entities, identities and identifiers [49]

According to Lily Bi, IAM is the way toward overseeing who approaches what data and for to what extent [52][53]. As per Hermans and ter Hart, IAM is the administration, procedures and supporting framework that oversees which clients gain admittance to data, IT assets and physical assets and what every client is approved to do with these assets [53]. The meaning of IAM utilized in this examination depends on the two definitions above in connection to the extent of this exploration. For this exploration, the accompanying meaning of IAM is utilized.

“The processes and technologies that manage the access of identities to digital resources and what authorization identities have over these resources.” To get a better overview of IAM, IAM can be divided into several parts. This research uses a model by Mather, Kumaraswamy and Latif [54][55] (Figure 07).

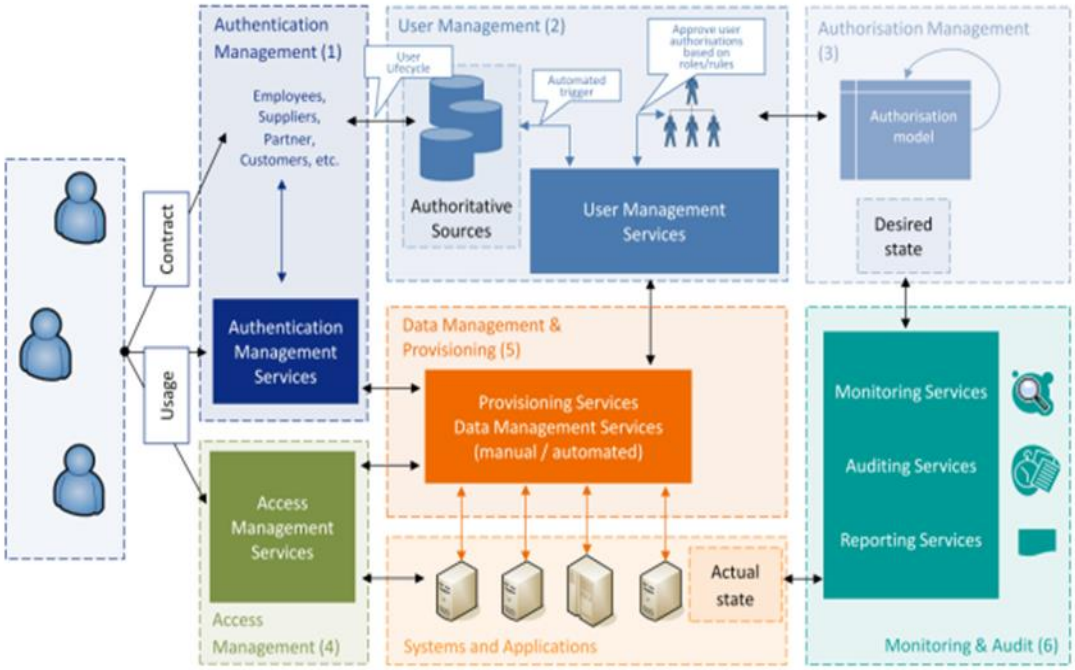


Figure 07: Enterprise IAM functional architecture [54]

The following definitions of the different parts of the model by Mather, Kumaraswamy, and Latif are used (Figure 07).

• Authentication management: Activities for the effective governance and management of the process ensuring that an entity is who or what he claims to be.

• User management: Taking measures for the effective guidance and managing identity life cycles.

• Authorization management: Measures taken to effectively managing identity life cycles and user guidance for selecting access rights that decide what resources an entity is permitted to access in accordance with the organization's rules.

• Access management: Enforcement of an organization's policies for access control in response to a request from an entity wanting to access a resource within the organization.

• Data management and provisioning: Management and propagation of identity and data for authorization to resources.

• Monitoring and auditing: Activities for monitoring, auditing and reporting compliance by users regarding access to resources within the organization based on the organization's policies.

In the conventional IT condition, clients must be included, changed or expelled from a framework and these clients can get to their approved assets. The general procedures of including, changing or evacuating a user don't change in a distributed computing condition. Clients still should be added to a framework to have the capacity to get to assets. Regardless of whether this framework is situated at a CSP, the clients must be perceived by the framework to get to its approved assets. Straightforward stated, the record of the representative still changes in an HR framework, a director still appoints or rejects a job and the verification gadget is still given to or withdrew from the user [55]. Nonetheless, contingent upon the model picked, parts of IAM are not overseen by the association itself. The equivalent applies to get to administration. A client still should give the validation gadget and is allowed or denied access to the asked for assets on the approvals. Regardless of whether the IAM procedures or parts of the IAM forms are not

dealt with, the association is constantly responsible for their IAM forms (Jansen and Grance, 2011).

Along these lines, it is fundamental to know which association controls of the IAM forms. In the accompanying areas, the progressions and dangers per part of IAM are analyzed. The IAM show, portrayed already, is utilized to characterize the distinctive parts of IAM. For every one of these parts of IAM the, beforehand depicted, distributed computing models are contrasted with the conventional IT condition [55]. The distinctions are inspected in the measure of control that an association has over that piece of IAM utilizing a distributed computing model. The more control the association has over its IAM the less effect a hazard has and the simpler it tends to be alleviated. For instance, if the association utilizes on-start confirmation to get to its assets it can without much of a stretch adjust the verification systems if they are shaky. Notwithstanding, if the association utilizes off-start confirmation the association isn't responsible for changes made to the verification systems. In the wake of looking at the distinctions for each distributed computing model contrasted with the conventional IT condition, the dangers are inspected. The accompanying danger measurements are investigated: Laws and Regulation, Data, Technology and Operational. The dangers are investigated for each piece of IAM. The effect of the hazard is reliant on whether the association utilizing the cloud administrations or the CSP possesses a piece of IAM. If the association is the proprietor of a piece of IAM, its level of control is higher, and the effect of the hazard is lower [55]. If the CSP is the proprietor of a piece of IAM, the level of control of the association utilizing the cloud administrations is lower and the effect of the hazard is higher.

5.5 MALICIOUS INSIDER

Redistributing of IT resources is certainly not very new thought in the business world. Recent years, we have encountered a genuine real increment in the number of organizations that choose to redistribute their IT resources. Cloud computing played a key role on this redistribution of IT resources. High scalability, flexibility and low cost are a portion of the components that make Cloud Computing so reliable. There are three essential administration models of cloud computing, to be specific: Software as a Service (SaaS), where software is offered by an outsider supplier, Platform as Service (PaaS), which encourages the development of new applications utilizing APIs managed and designed remotely and Infrastructure as a service (IaaS) [57], which gives disconnected equipment and working frameworks abilities, basically through virtualization. This type of distribution of IT resources influences the risk of fake or malicious profiles but with proper administrative measure this type of danger can be mitigated [58] [65].

Moreover, specialists have pointed towards the security issues that cloud computing may acquaint with basic foundations [59] [60] [61]. Regardless of whether the company decides not to use cloud computing for their IT resources distribution, it will even be threat if any person from the company use any of the services like email, video streaming that uses cloud computing using company infrastructure. This type of incidents can be considered the insider risk, and it is characterized as a man who has the proper access rights to a data framework and abuses his benefits [62] [63].

For instance, a formal employee of the company who has been terminated and have revenge mentality towards the company. Though all the credentials of that employee had terminated already yet he/she has knowledge regarding the Its redistribution of the company can pose serious threat and can be treated as insider threat. Alleviation of this issue is regularly confused, as an insider can center around an assortment of target frameworks and arrange his/her attack persuaded by a few reasons [64], from individual benefit to revenge [65]. The insider has the benefit of time, to think about the data framework and send a genuine attack.

5.5.1 INSIDER THREAT IN THE CLOUD PROVIDER

This is the worst outcome imaginable for both cloud suppliers and cloud customers, Considering the insiders job in the cloud supplier company, the insider can utilize his/her approved client rights to get to delicate information. An administrator in charge of performing consistent reinforcements of the frameworks where customer data is facilitated, could easily manipulate or save some of the sensitive customer data. Distinguishing such corrupted access to information, can be very difficult. Contingent upon the insider's thought processes, the after effect of such an attack in a cloud framework will change from information spillage to extreme defilement of the affected frameworks and information [65]. In any case, the business affect for the supplier will be huge. All basic cloud composes (IaaS, PaaS, SaaS) are similarly influenced by insider attacks if the insider has access to the datacenters or cloud administration frameworks. The choice to distribute IT resources especially in cloud is combined with an inborn danger of presenting touchy information to an Outside Company, however cloud computing separates since it offers a solution by means of IaaS and PaaS. Subsequently, cloud computing worldview could be used to re-appropriate huge parts of the framework rather than administrations.

5.5.2 INSIDER THREAT IN THE CLOUD OUTSOURCER

The opposite situation to the previously we discussed is when the insider is a worker of an association, which has moved the part of or the entire IT framework into the cloud. This could be considered as a customary insider issue. But we can consider that there are a few noticeable contrasts. Firstly, cloud service providers can detect the work of different doubtful employees. But tracing that type of customer is tricky at times because to detect any misuse both the cloud infrastructure and the individual company's workstation data needed. Moreover, doubtful user profiling becomes more difficult as the user's behavior in the cloud must be included as a model parameter. Secondly, cloud utilization along with broad logging of client activities could prompt valuable information. This information could be utilized to portray client's activities in cloud environment, which may prompt better client profiling. On the contrary, these models have not been connected or considered inside the setting of cloud computing, we can just guess about the outcomes [65].

CHAPTER 06: ATTACK TECHNIQUES AND METHODS

6.1 METHODS AND TOOLS

Compared to other kinds of cyber-attacks, denial of service attacks (DoS) attacks are messy and very difficult to pull off as they don't make much sense from a financial perspective. Bur instantly a DoS attack might bring down the victim resources or a small online web server.

A denial-of-service (DoS) attack can carrying out and perform more than one way and in many manners. The attackers are relying then in Botnets to execute DDoS attacks. A botnet is a collection connected devices that have been infected with malware, where it is controlled by a single attacker and used to perform distributed denial-of-service attack.[66]

The hackers who don't have any access to botnets are relying on their own machines with some specialized tools to execute a DoS attack. Although some methods are not very powerful but easier to execute and can simultaneously attack a particular victim or a website.

Before executing a DoS attack the attackers take some primary steps, such as monitoring the network activities, identifying the vulnerabilities of the victim system and identifying the open ports by scanning them using some scanning tools.

6.2 PERFORMING DoS ATTACKS

6.2.1 Airodump-ng

Airodump-ng is used for packet capturing of raw 802.11 frames and is particularly suitable for collecting WEP IVs (Initialization Vector) for the intent of using them with aircrack-ng. [67]

Usage

We have used airodump-ng to send a deauthentication request to our local router.

Scenario 01:

To attempt a DoS attack to make the local router unavailable to internet, as well as to interrupt intranet communication between the host machine.

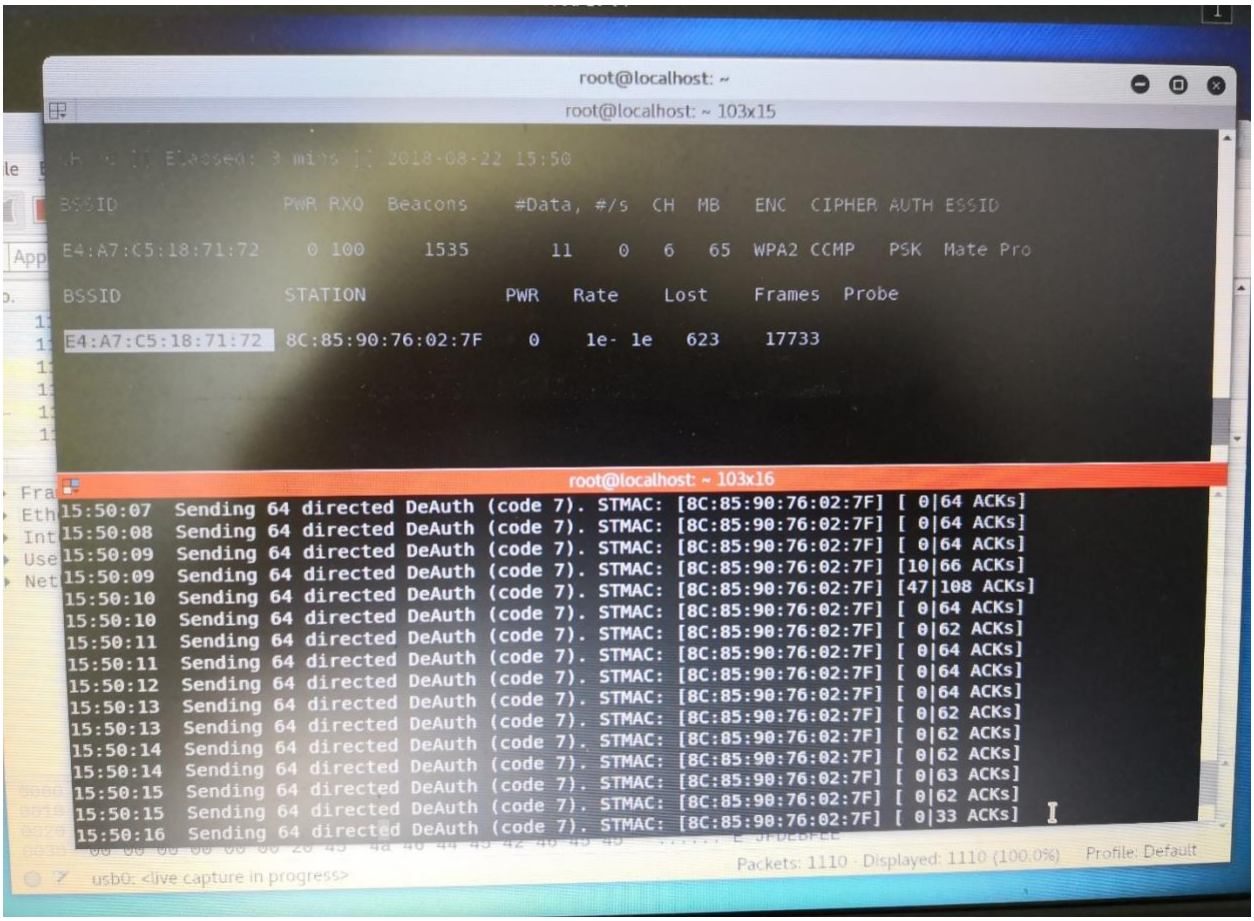
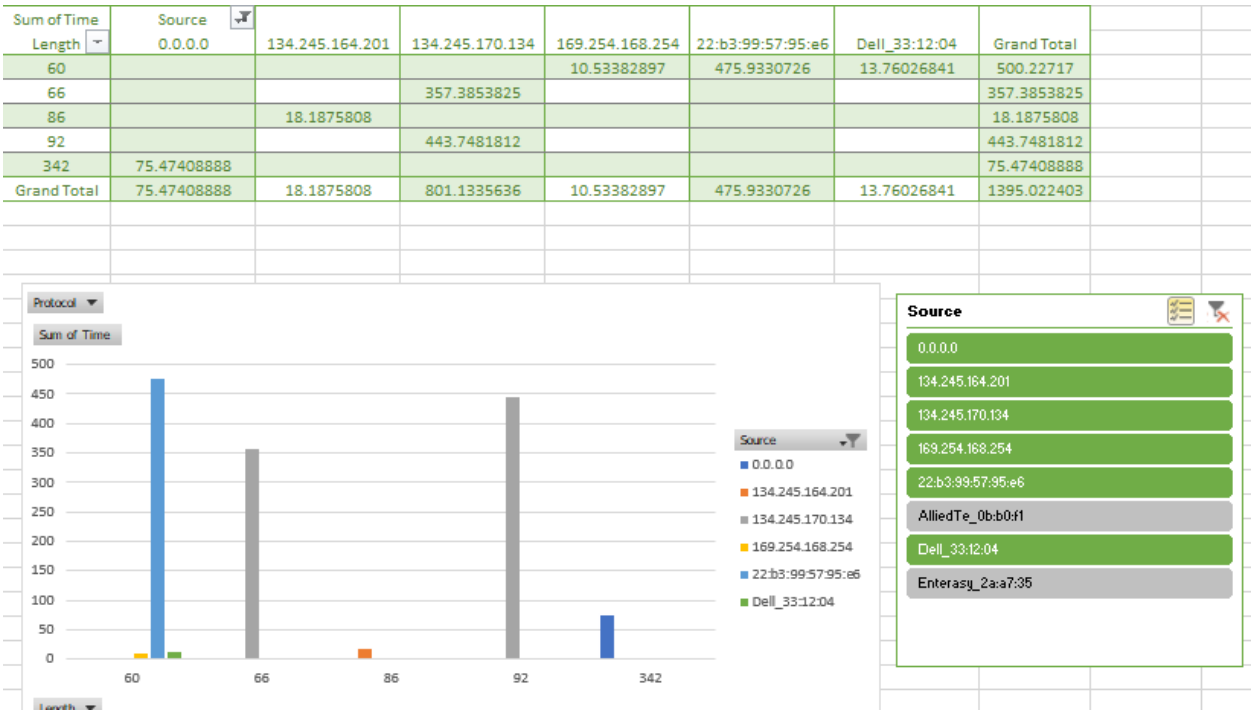


Figure 08: DoS de-authentication in progress in a router interface.

Figure shows that, the attacker sending a ‘deauthenticaiton’ request to the router. The router mac address is **8C:85:90:76:02:7F.**

We have performed the experiment for one minute and got huge packet of data. We have captured and analyzed the data packet with the tool named ‘wireshark’. The following image describes the summary of our collected data.



Sum of Time / Length	Source 0.0.0.0	134.245.164.201	134.245.170.134	169.254.168.254	22:b3:99:57:95:e6	Dell_33:12:04	Grand Total
60				10.53382897	475.9330726	13.76026841	500.22717
66			357.3853825				357.3853825
86		18.1875808					18.1875808
92			443.7481812				443.7481812
342	75.47408888						75.47408888
Grand Total	75.47408888	18.1875808	801.1335636	10.53382897	475.9330726	13.76026841	1395.022403

Figure 09: Data summary after a DoS de-authentication in a router interface.

Here,

134.245.164.201 is our router IP address.

134.245.170.134 is the attacker machine.

169.254.168.254 is the service provider IP address.

Syntax:

Airodump-ng -c 12 –bssid 8C:85:90:76:02:7F wlan0

-c 12 channel number of the target mac address

8C:85:90:76:02:7F target mac address

Wlan0 interface

Aireplay-ng -0 0 -a 8C:85:90:76:02:7F wlan0

-0 0 for an unlimited loop until the operation is not manually stopped.

- a to specify the mac address of the access point.

Scenario 02:

To attempt a DoS attack to make a specific host to connect the router and access the internet.

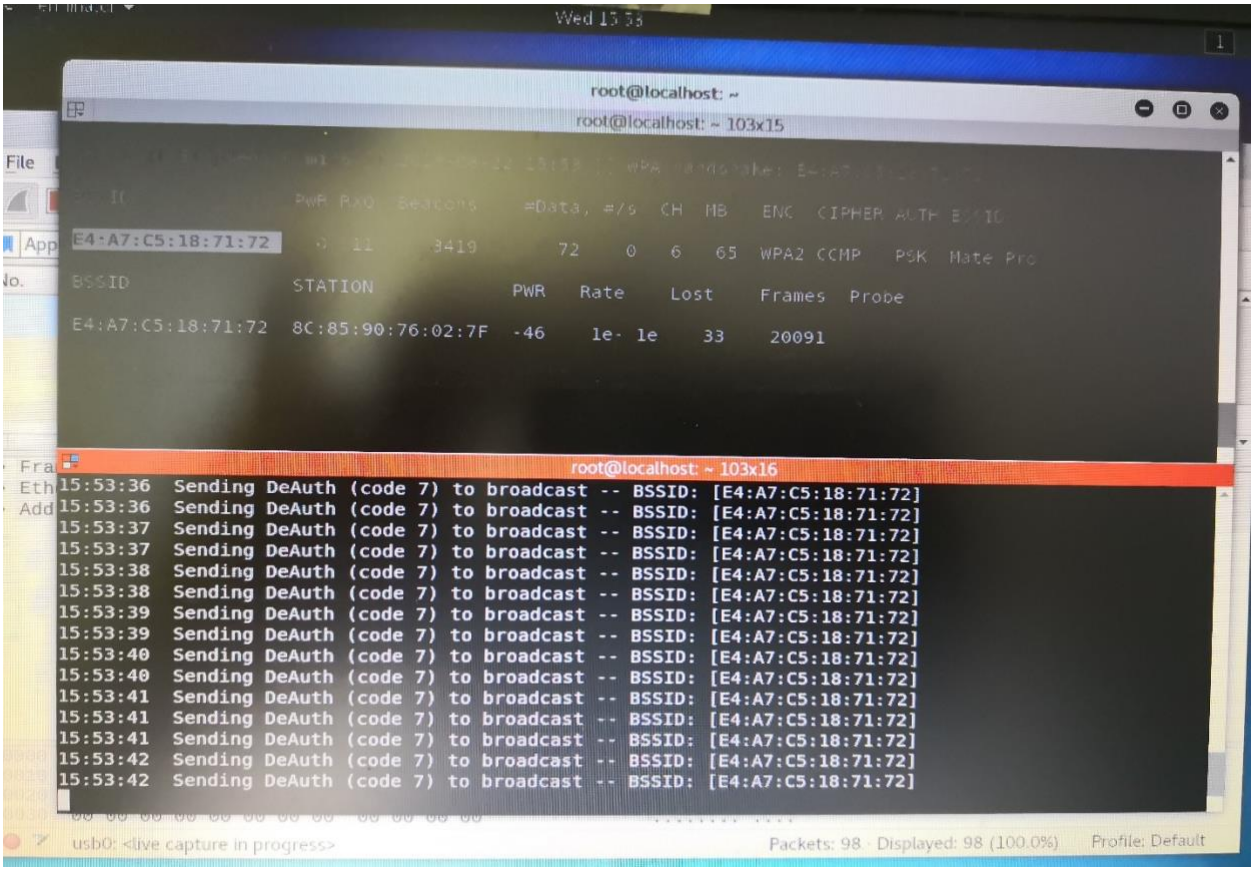


Figure 10: DoS de-authentication in progress for a specific device.

Figure shows that, the attacker sending a ‘deauthenticaiton’ request to a host device inside a network. The router mac address is **8C:85:90:76:02:7F** and the host mac address is **E4:A7:C5:18:71:72.**

Syntax:

Airodump-ng -c 12 –bssid E4:A7:C5:18:71:72 wlan0

-c 12 channel number of the target mac address

E4:A7:C5:18:71:72 target mac address

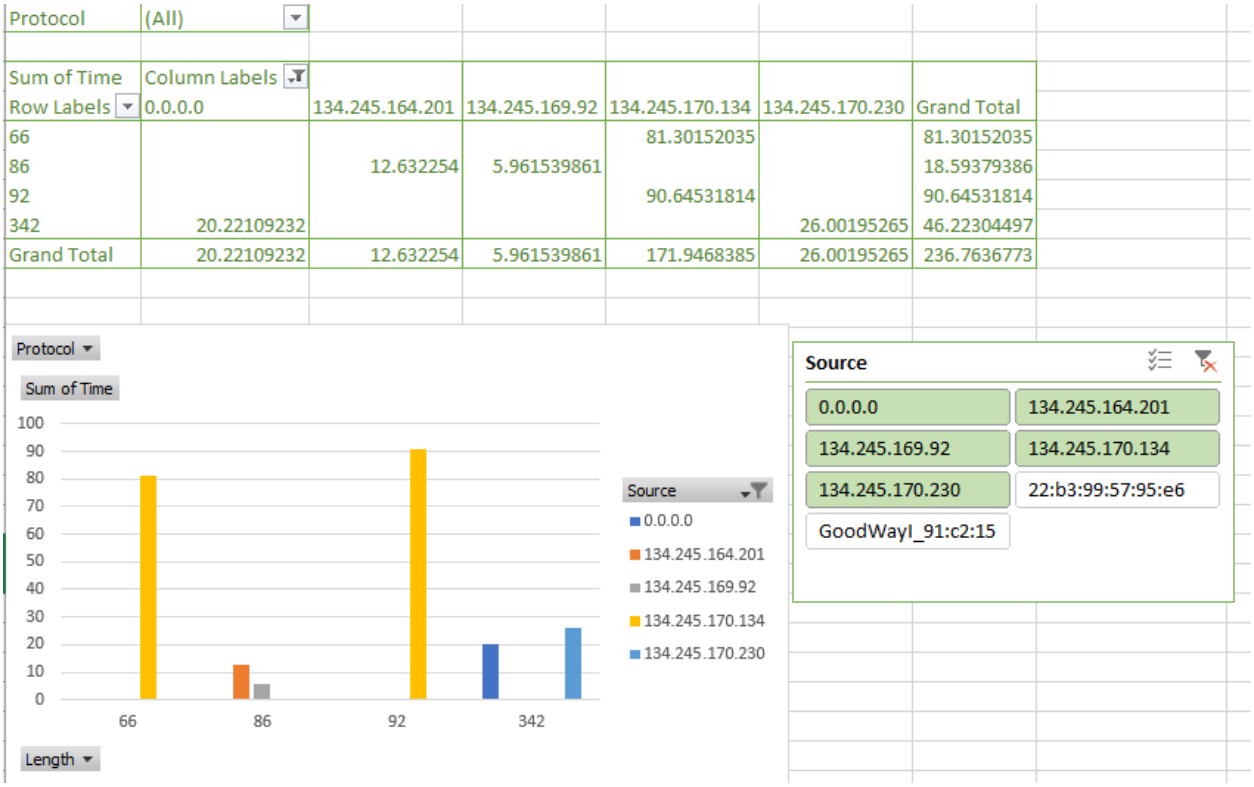
Wlan0 interface

Aireplay-ng -0 0 -c E4:A7:C5:18:71:72 wlan0

-0 0 for an unlimited loop until the operation is not manually stopped.

- c to specify the mac address of the host device.

We have performed the experiment for one minute and got huge packet of data. We have captured and analyzed the data packet with the tool named ‘wireshark’. The following image describes the summary of our collected data.



Protocol	(All)					
Sum of Time	Column Labels					
Row Labels	0.0.0.0	134.245.164.201	134.245.169.92	134.245.170.134	134.245.170.230	Grand Total
66				81.30152035		81.30152035
86		12.632254	5.961539861			18.59379386
92				90.64531814		90.64531814
342	20.22109232				26.00195265	46.22304497
Grand Total	20.22109232	12.632254	5.961539861	171.9468385	26.00195265	236.7636773

Figure 11: Data summary after a DoS de-authentication for a specific device.

Here,

134.245.164.201 is our router IP address.

134.245.170.134 is the attacker machine.

134.245.170.230 is the victim device.

169.254.168.254 is the service provider IP address.

6.2.2 WI-FI JAMMER

Websploit Framework is an open source tool that is designed for vulnerability analysis and penetration testing for web applications. This framework provides four categories of modular such as web modules, network modules, exploit modules and wireless modules.[73]

Some useful and effective features of Websploit framework are:

- Social Engineering Works
- Support Network Attacks
- Scan, Crawler & Analysis Web
- Php my admin scanner
- apache directory scanner
- ARP Dos Attack
- Web Killer Attack
- Fake Update Attack
- WiFi Honeypot
- WiFi Jammer
- WiFi Dos
- MITM – Man in The Middle Attack
- Bluetooth POD Attack
-

The websploit "wifi_jamming" is one of many possible denial of service (DoS) attacks against a wifi network. Rather than overpowering the signal wifi_jamming disconnected all devices from the access point. This attack has the advantage against any wifi network, without needing to be authenticated to the network.

The process is described below:

At first, we have to start 'Websploit' framework with the following command in a terminal:

- Websploit
- Show modules
- Use wifi/wifi_jammer
- Show options
- set BSSID [BSSID of your target]
- set ESSID [ESSID of your target]
- set channel [channel number]
- run

Figure 12: Websploit wifi_jammer Attack screenshot.

After performing the wifi/wifi_jammer attack we have generated the data given below. And with the help of Wireshark we were able to convert our data as a CSV file so that we can do further analysis our data with Excel and understand our required insights.

No.	Time	Source	Destination	Protocol	Length	Frame	Info
1	0	Sercomm_ab:03	Broadcast	802.11	53	Yes	Deauthentication, SN=3286, FN=0, Flags=.....[Malformed Packet]
2	0.000747	Sercomm_ab:03	Broadcast	802.11	53	Yes	Deauthentication, SN=3287, FN=0, Flags=....., SSID=Broadcast
3	0.001367	Sercomm_ab:03	Broadcast	802.11	53	Yes	Deauthentication, SN=3027, FN=0, Flags=....., SSID=Broadcast
4	0.001536	Sercomm_ab:03	Broadcast	802.11	52	Yes	Deauthentication, SN=3031, FN=0, Flags=....., SSID=Broadcast
5	0.001552	Sercomm_ab:03	Broadcast	802.11	52	Yes	Deauthentication, SN=3291, FN=0, Flags=....., SSID=Broadcast
6	0.002128	Sercomm_ab:03	Broadcast	802.11	53	Yes	Deauthentication, SN=3028, FN=0, Flags=....., SSID=Broadcast
7	0.002765	Sercomm_ab:03	Broadcast	802.11	53	Yes	Deauthentication, SN=3288, FN=0, Flags=....., SSID=Broadcast
8	0.003497	Sercomm_ab:03	Broadcast	802.11	53	Yes	Deauthentication, SN=3029, FN=0, Flags=....., SSID=Broadcast
9	0.003616	Sercomm_ab:03	Broadcast	802.11	52	Yes	Deauthentication, SN=3292, FN=0, Flags=....., SSID=Broadcast
10	0.00363	Sercomm_ab:03	Broadcast	802.11	52	Yes	Deauthentication, SN=3032, FN=0, Flags=....., SSID=Broadcast
11	0.004127	Sercomm_ab:03	Broadcast	802.11	53	Yes	Deauthentication, SN=3289, FN=0, Flags=....., SSID=Broadcast
12	0.004752	Sercomm_ab:03	Broadcast	802.11	53	Yes	Deauthentication, SN=3030, FN=0, Flags=....., SSID=Broadcast
13	0.005502	Sercomm_ab:03	Broadcast	802.11	53	Yes	Deauthentication, SN=3290, FN=0, Flags=....., SSID=Broadcast
14	0.005684	Sercomm_ab:03	Broadcast	802.11	52	Yes	Deauthentication, SN=3033, FN=0, Flags=....., SSID=Broadcast
15	0.005718	Sercomm_ab:03	Broadcast	802.11	52	Yes	Deauthentication, SN=3293, FN=0, Flags=....., SSID=Broadcast
16	0.006136	Sercomm_ab:03	Broadcast	802.11	53	Yes	Deauthentication, SN=3031, FN=0, Flags=....., SSID=Broadcast
17	0.006878	Sercomm_ab:03	Broadcast	802.11	53	Yes	Deauthentication, SN=3291, FN=0, Flags=....., SSID=Broadcast
18	0.007494	Sercomm_ab:03	Broadcast	802.11	53	Yes	Deauthentication, SN=3292, FN=0, Flags=....., SSID=Broadcast
19	0.007788	Sercomm_ab:03	Broadcast	802.11	52	Yes	Deauthentication, SN=3034, FN=0, Flags=....., SSID=Broadcast
20	0.00781	Sercomm_ab:03	Broadcast	802.11	52	Yes	Deauthentication, SN=3294, FN=0, Flags=....., SSID=Broadcast

Figure 13: Wi-FI Jammer de-authentication raw data.

Upon Excel pivot analysis of our raw data we were able to generate the table given below:

Sum of Time	Column Labels					
Row Labels	86:25:19:0e:62:f3	MurataMa_06:b5:e1	Sercomm_7e:32:6a	Sercomm_7e:32:6b	Sercomm_ab:03:d6	Grand Total
52					0.991481473	0.99148147
53					1.066596891	1.06659689
56		0.041407559				0.04140756
261				0.034474266		0.03447427
267			0.028237056			0.02823706
272	0.045669489					0.04566949
273					0.010425506	0.01042551
Grand Total	**0.045669489**	**0.041407559**	**0.028237056**	**0.034474266**	**2.06850387**	**2.21829224**

Figure 14: Data summary after a Wi-Fi de-authentication process.

This Chart shows our pivot table analysis values:

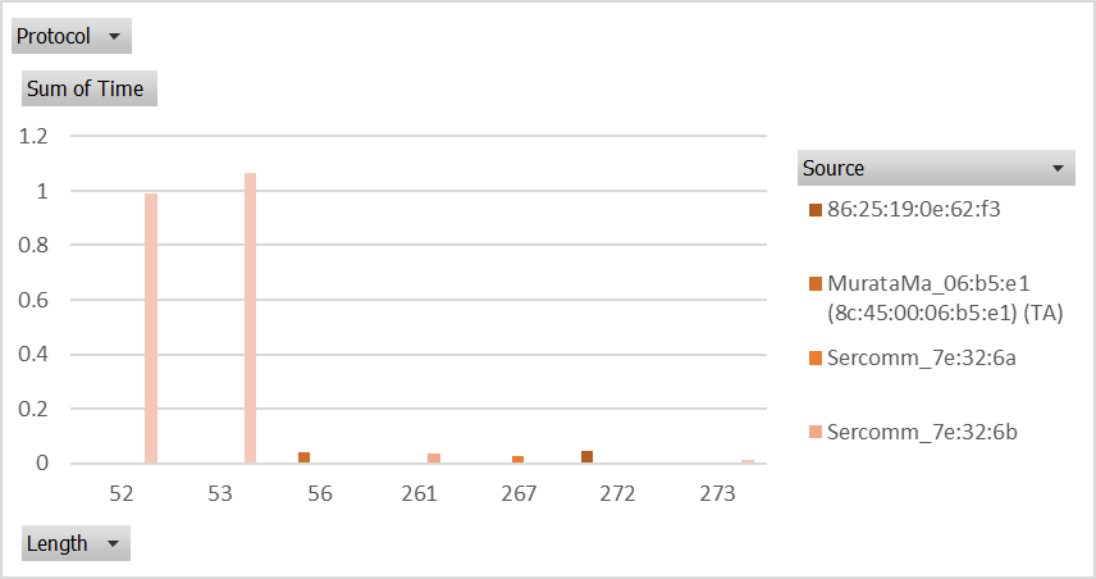


Figure 15: Pivot analysis of attack data (Wi-Fi Jammer).

6.2.3 PENTMENU

Pentmenu is a penetration testing and a bash script tool which is inspired by pent box. Pentmenu is designed in a simple way to implement various penetration functions and offers several types of DoS attack. This attacking tool is easy to use but very effective to perform a DoS attack, and it is mostly used in Linux based resources. [68] A penetration tester just needs to download the bash script, make it executable and then run it with some simple command lines.

The bash script tool has some requirements: [68]

- bash
- curl
- nmap
- whois
- hping3
- netcat
- openssl

Download and uses

Download pentmenu the script by executing this command in the terminal:

> git clone https://github.com/GinjaChris/pentmenu.git

To go to the directory type:

>cd pentmenu

>ls

Make it executable and run:

> chmod +x ./pentmenu

>./pentmenu

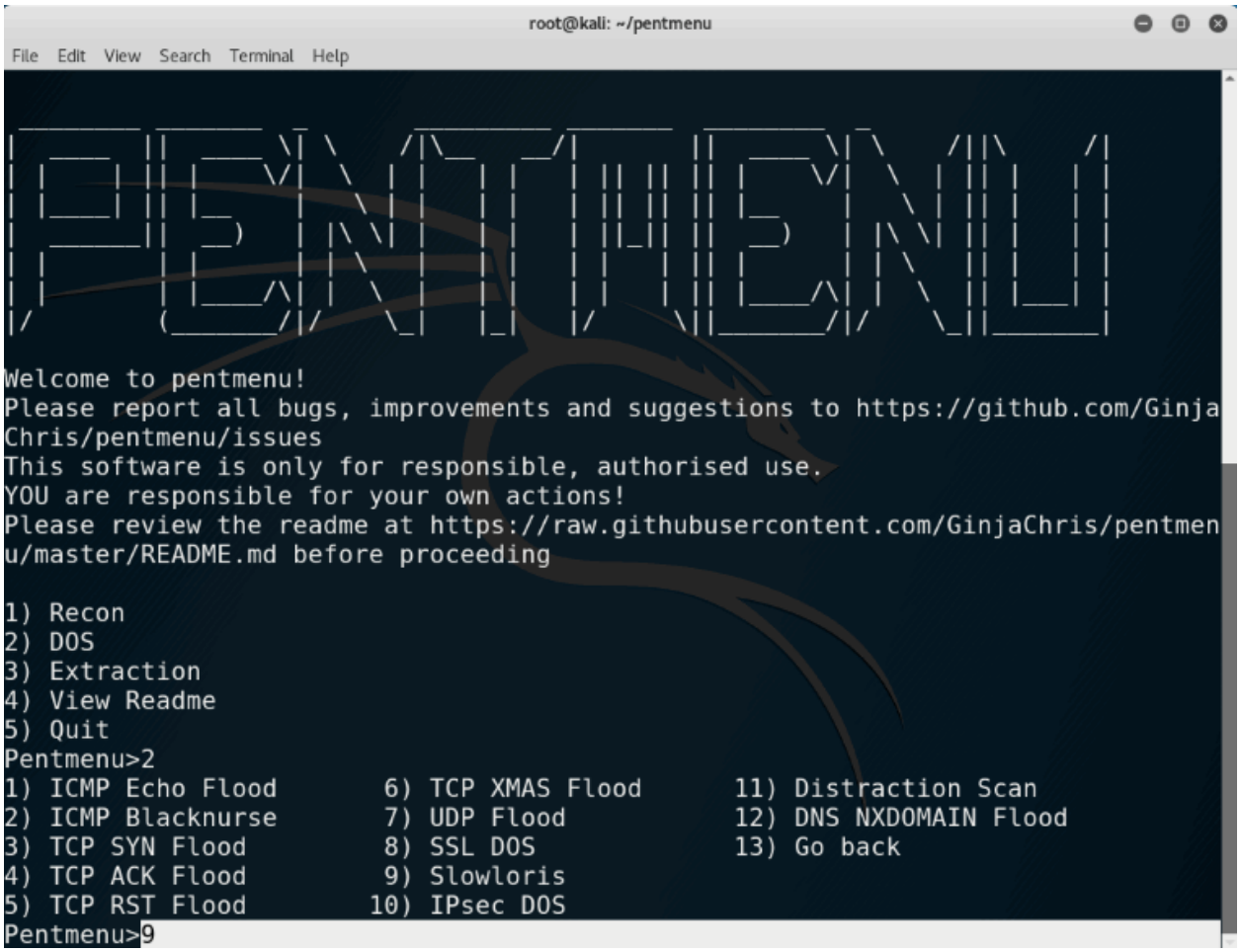


Figure 16: Pentmenu penetration testing and a bash script tool interface.

More details

Recon Modules of Pentmenu [68]

- **Show IP:** To show local interfaces type ifconfig or uses curl to perform a lookup of your external IP.
- **DNS Recon:** It's a passive recon which perform a whois lookup to find out the hostname of the target and a DNS lookup of the target. It performs a lookup against ipinfo.io when the whois is not available.
- **Ping Sweep:** Nmap or zenmap is used to perform an ICMP echo request against the victim network.

- **Network Recon:** Uses nmap or zenmap to identify and find out open ports, detecting operating system including the version of the target machine. Prior as part of this scan nmap will not perform a ping sweep.
- **Stealth Scan:** Uses nmap port scanner to identify and scan the TCP open ports using TCP SYN scan. In this scanning nmap will not perform a ping sweep and can take a long time to finish.
- **UDP scan:** Uses nmap/zenmap port scanner to identify and scan the UDP open ports of the victim.
- **Check Server Uptime:** Calculates accuracy and the maximum uptime of the victim system or a website server by querying an open TCP port with hping3. The results may vary from one machine to another.

The bash script tool is specially used to execute some DoS attacks:

- TCP SYN Flood: It sends TCP SYN packets using hping3 and where hping3 can send packets as fast as possible. This bash script uses the nmap and nping utility instead of hping3 if hping3 is not available. Hping3 has some options to use a source IP or real IP of an attacker or can use a random source IP for sending the packets. The attacker can optionally add data to the SYN packets where all SYN packets have the fragmentation bit set.

- UDP Flood: It works likely the TCP SYN flood but instead of TCP SYN it sends UDP packets to the target host. Hping3 is used to send UDP packets and like the TCP SYN it uses nmap-nping if hping3 is not found. It has no option to add data to the packets, but it is a good way to check access points.

- SSL DOS: It uses open SSL to execute and attempt to a DoS attack to the target ports. It causes the victim server to make an expensive handshake calculation by opening many connections. This type of DoS attacks cannot stop immediately, and it can be brutally effective.

Slowloris: Slowloris attack uses netcat and send HTTP Headers to the victim ports. This attack is effective against many HTTP servers only if the server does not limit the time to send a HTTP request and it can open the connections for a long time. Therefore, this attack can be implemented by using clearly identifiable headers.

- The idea behind the slowloris attack is to send headers slowly, but not so slow that the servers idle timeout closes the connection. Therefore, the protections against the slowloris DoS attacks are (1) limiting the number of TCP connections per client. This will prevent a single machine from making the server unavailable. (2) Limiting the available time to send a complete HTTP request to the victim server. Sends the HTTP request slowly so that the server's connection will be timeout.

- Distraction Scan: This is not depending on a DoS attack but using hping3 and can simply launch multiple TCP SYN scans from a spoofed IP.

Some extraction modules of pentmenu bash script:

- ✓ File extraction via ICMP – to send data with ICMP packets uses hping.
- ✓ File receipt via ICMP – to listen for ICMP packets and record the data to an output file uses hping.
- ✓ Listener –to open a listener on a configurable TCP or UDP port uses netcat.

6.2.3.1 Pentmenu UDP Flood:

Upon devising our attack with 'Pentmenu' software we have generated the data given below. And with the help of Wireshark we were able to convert our data as a CSV file so that we can further analysis our data with Excel and understand our needed insights.

1	0	53.36.83.171	192.168.2.104	QUIC	46	Yes
2	0.000108874	197.221.96.114	192.168.2.104	QUIC	46	Yes
3	0.000125332	60.187.191.139	192.168.2.104	QUIC	46	Yes
4	0.00013588	212.240.11.225	192.168.2.104	QUIC	46	Yes
5	0.000144667	139.223.175.174	192.168.2.104	QUIC	46	Yes
6	0.000152868	64.238.28.235	192.168.2.104	QUIC	46	Yes
7	0.000161751	206.45.228.240	192.168.2.104	QUIC	46	Yes
8	0.000172319	60.163.1.25	192.168.2.104	QUIC	46	Yes
9	0.000181826	46.240.243.11	192.168.2.104	QUIC	46	Yes
10	0.000190835	251.25.19.23	192.168.2.104	QUIC	46	Yes
11	0.000199714	28.73.92.97	192.168.2.104	QUIC	46	Yes
12	0.000208538	170.206.163.135	192.168.2.104	QUIC	46	Yes
13	0.000217028	163.135.130.22	192.168.2.104	QUIC	46	Yes
14	0.000225145	118.171.115.19	192.168.2.104	QUIC	46	Yes
15	0.000234834	72.53.159.191	192.168.2.104	QUIC	46	Yes
16	0.000244174	46.102.102.104	192.168.2.104	QUIC	46	Yes
17	0.000252488	224.163.34.62	192.168.2.104	QUIC	46	Yes
18	0.000260889	235.221.37.206	192.168.2.104	QUIC	46	Yes
19	0.000269131	184.198.137.17	192.168.2.104	QUIC	46	Yes

Figure 17: Pentmenu UDP-Flood raw data.

Upon Excel pivot analysis of our raw data we were able to generate the table given below:

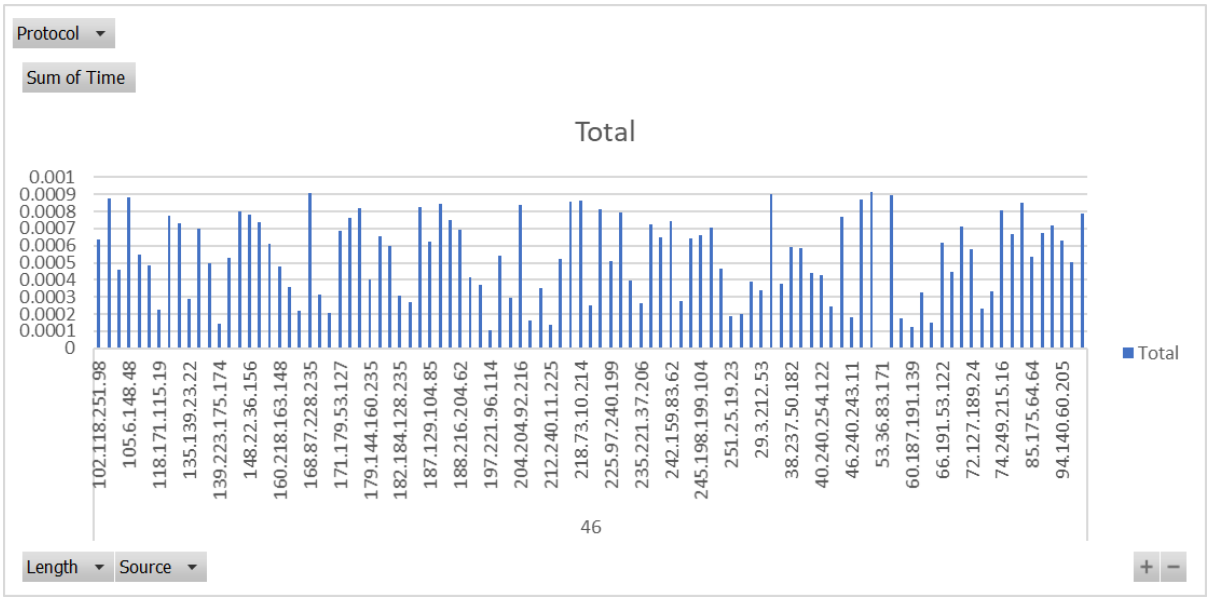


Figure 18: Pivot analysis of attack data (Pentmenu UDP-Flood).

6.2.3.2 Pentmenu TCP SYN:

Upon devising our attack with pentmenu software we have generated the data given below. And with the help of Wireshark we were able to convert our data as a CSV file so that we can further analysis our data with Excel and understand our needed insights.

Time	Source	Destination	Protocol	Length	Frame
0	98.25.181.203	192.168.2.104	IPv4	50	Yes
0.000048369	98.25.181.203	192.168.2.104	IPv4	50	Yes
0.000059325	98.25.181.203	192.168.2.104	IPv4	50	Yes
0.000068679	98.25.181.203	192.168.2.104	IPv4	50	Yes
0.000077888	98.25.181.203	192.168.2.104	IPv4	50	Yes
0.000087029	98.25.181.203	192.168.2.104	IPv4	50	Yes
0.0000964	98.25.181.203	192.168.2.104	IPv4	50	Yes
0.000105974	98.25.181.203	192.168.2.104	IPv4	50	Yes
0.000115775	98.25.181.203	192.168.2.104	IPv4	50	Yes
0.000124901	98.25.181.203	192.168.2.104	IPv4	50	Yes
0.000134034	98.25.181.203	192.168.2.104	IPv4	50	Yes
0.000143332	98.25.181.203	192.168.2.104	IPv4	50	Yes
0.000152994	98.25.181.203	192.168.2.104	IPv4	50	Yes
0.000162031	98.25.181.203	192.168.2.104	IPv4	50	Yes
0.000171063	98.25.181.203	192.168.2.104	IPv4	50	Yes
0.00018002	98.25.181.203	192.168.2.104	IPv4	50	Yes
0.000189073	98.25.181.203	192.168.2.104	IPv4	50	Yes
0.000198115	98.25.181.203	192.168.2.104	IPv4	50	Yes
0.000207572	98.25.181.203	192.168.2.104	IPv4	50	Yes

Figure 19: Pentmenu TCP SYN raw data.

Upon Excel pivot analysis of our raw data we were able to generate the table given below:

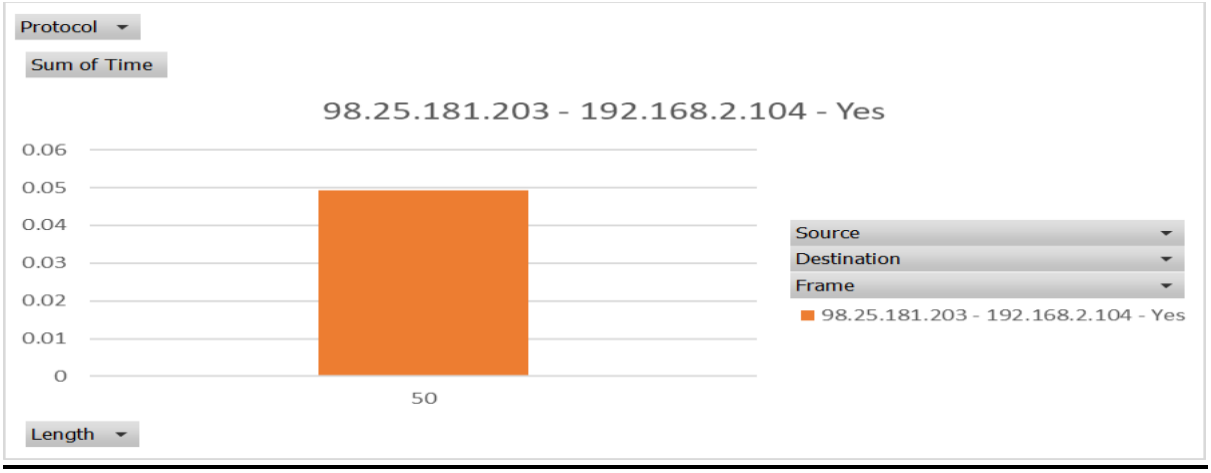


Figure 20: Pivot analysis of attack data (Pentmenu TCP SYN-Flood).

6.2.4 LOW ORBIT ION CANON (LOIC)

Low Orbit Ion Cannon is an application commonly used to launch denial of service attacks (DoS) and distributed denial of service attacks (DDoS). The original LOIC Tool was written in C#, developed by Praetox Technology and use by members of hacktivist group Anonymous as well as users of the 4Chan forums. [69]

The idea behind LOIC is that it has become an open-source tool and is now mostly used with malicious intent. LOIC is a user-friendly tool that allow anyone to execute a DoS attack even if he has no idea how to use it. The pros of LOIC is that it is available for windows, Linux and mac OS. The opensource tool is widely available for download and provide a type of version based on the DoS attacks. The users can use a JavaScript version tool called JS LOIC to launch a DoS attack from a web browser. It has also a web version tool known as the Low Orbit Web Cannon.

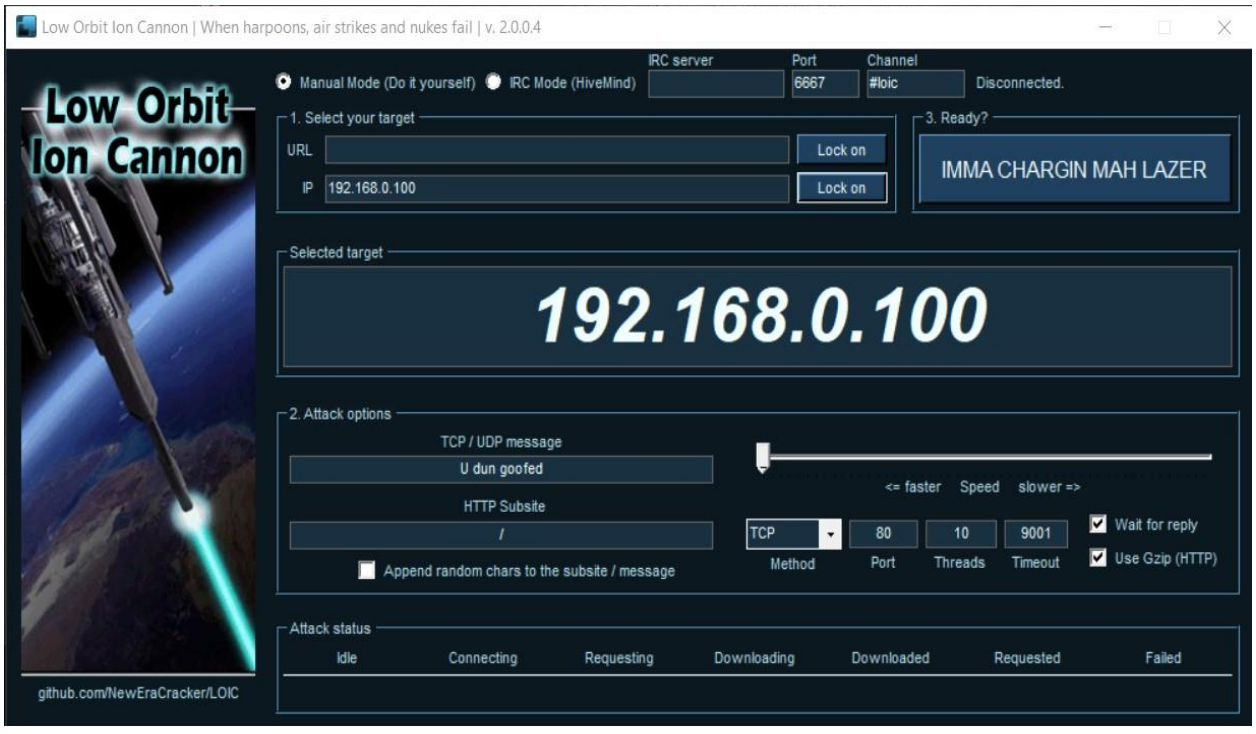


Figure 21: Low Orbit Ion Canon interface.

The tool can perform simple DoS attack by sending a set of TCP requests or UDP requests or HTTP requests to a target host.

Working principle of LOIC

LOIC allows a user to select a target host with the goal of disrupting the target service. It works by flooding a victim server by sending TCP, UDP, or HTTP packets where the user can control the destination port number, the content of the messages and the number of concurrent threads. LOIC tool has two modes of operation,

- ✓ Manual mode – allows a user to fill up the target address and other parameters.
- ✓ Automatic mode – allows a user to attack remotely.

The current version of LOIC uses “operation payback” that allows the tool to be remotely controlled, using the internet relay chat (IRC). In LOIC the three types of attacks are similar but each using a different packet type and sends continuously a pre-defined string. The LOIC generates HTTP GET requests based on random URLs Once the HTTP attack has been started. The source machine opens many connections as possible to the target host by trying to access the target URL.

Upon Excel pivot analysis of our raw data we were able to generate the table given below:

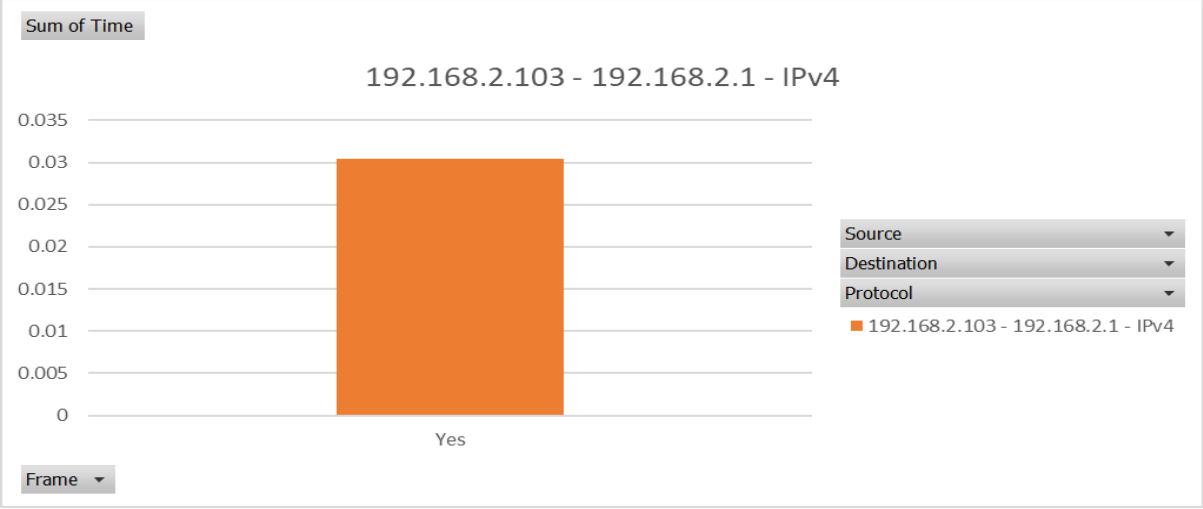


Figure 22: Pivot analysis of attack data (LOIC).

6.2.5 XEROSPLOIT

Xerospoloit is a tool that allows a user to perform denial of service attacks, man in the middle attacks for the testing purposes. Xerosploit is a penetration testing toolkit that was committed by LionSec whose goal is to perform MITM attacks and also allows to carry out denial of service attacks and port scanning. [70] The tool has driftnet modules which capture images and also used in performing Injection attacks.

Download and Installation

- git clone https://github.com/LionSec/xerosploit
- cd xerosploit && sudo python install.py
- ./xerosploit.py

Xerosploit toolkit has some dependencies: [70]

- Nmap
- hping3
- build-essential
- ruby-dev
- libpcap-dev
- libgmp3-dev
- tabulate
- terminaltables

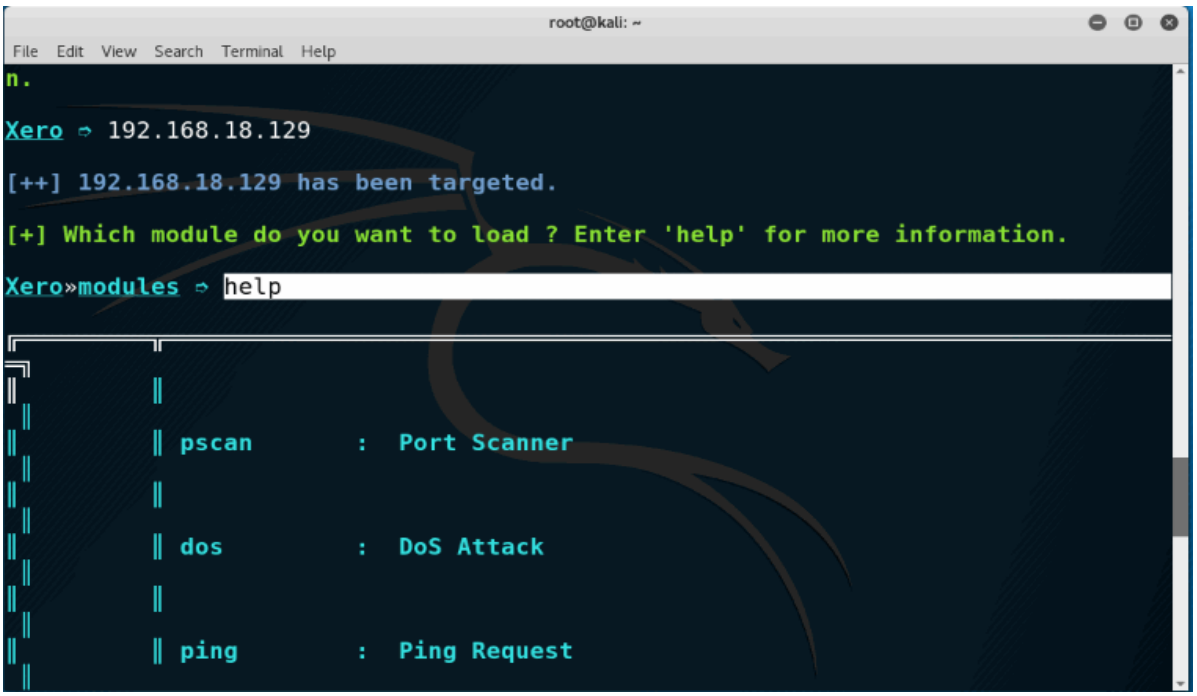


Figure 23: Xerosploit Penetration toolkit interface.

Upon devising our attack with ‘Xerosploit’ software we have generated the data given below. And with the help of Wireshark we were able to convert our data as a CSV file so that we can further analysis our data with Excel and understand our required insights.

1	0	248.100.34.67	192.168.2.1	FTP	174	Yes
2	0.000038333	67.68.88.67	192.168.2.1	FTP	174	Yes
3	0.000047079	216.100.58.174	192.168.2.1	FTP	174	Yes
4	0.000054538	9.174.120.103	192.168.2.1	FTP	174	Yes
5	0.000061721	241.185.100.80	192.168.2.1	FTP	174	Yes
6	0.000068847	139.25.47.18	192.168.2.1	FTP	174	Yes
7	0.000075657	159.156.53.190	192.168.2.1	FTP	174	Yes
8	0.000082721	211.119.190.107	192.168.2.1	FTP	174	Yes
9	0.000089885	100.90.27.68	192.168.2.1	FTP	174	Yes
10	0.000096754	139.180.169.164	192.168.2.1	FTP	174	Yes
11	0.000103662	57.251.248.164	192.168.2.1	FTP	174	Yes
12	0.000110394	62.75.153.222	192.168.2.1	FTP	174	Yes
13	0.000117222	205.9.81.148	192.168.2.1	FTP	174	Yes
14	0.000125083	72.202.219.70	192.168.2.1	FTP	174	Yes
15	0.000132153	230.222.160.106	192.168.2.1	FTP	174	Yes
16	0.000138921	202.108.174.111	192.168.2.1	FTP	174	Yes
17	0.000146118	167.2.79.193	192.168.2.1	FTP	174	Yes
18	0.000153286	241.118.156.25	192.168.2.1	FTP	174	Yes
19	0.000160149	228.212.140.196	192.168.2.1	FTP	174	Yes
20	0.000166819	97.115.131.220	192.168.2.1	FTP	174	Yes

Figure 24: DoS attack (raw data) in a router interface using 'Xerosploit'.

This Chart shows our pivot table analysis values:

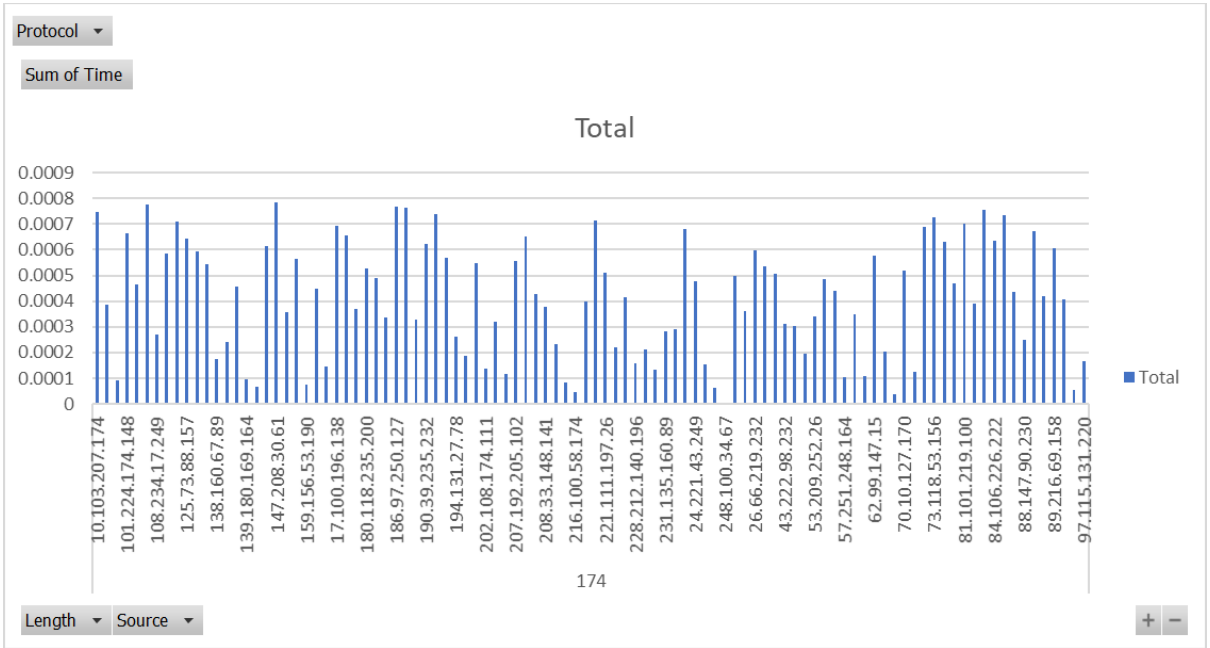


Figure 25: Pivot analysis of attack data (Xerosploit)

CHAPTER 07: VULNERABILITY DETECTION AND MITIGATION

The common nature of cloud computing such as elasticity, openness and a large amount of data makes itself more attracted to attackers. Virtualization, flexibility and scalability have amplified the security threats a bit more. Attackers can exploit vulnerabilities anonymously from any geographical location. Moreover, the required tools and codes are available, and it does not need much skills to execute the vulnerabilities. Before we deep dive about mitigation, we would like to discuss some preliminary countermeasures which can be taken at first attempt to secure the cloud interface.

7.1 FIREWALL AND INTRUSION DETECTION SYSTEM

Firewalls may be able to mitigate or stop the incoming vulnerabilities, but it has no effect on internal attacks where the internal cloud users attempt to gain unauthorized privileges. For this reason, Intrusion Detection System (IDS) has been designed for cloud computing and it is classified into four main categories: [74]

01. **Host-based IDS (HIDS),** can monitor and analyze log files, security access and user login information to detect intrusive behavior.
02. **Network-based IDS (NIDS),** can monitor IP and transport layer headers with behaviour being compared with previously observed behavior in real time.
03. **Hypervisor-based IDS (HyIDS),** allows users to monitor and analyze communication between virtual machines, within the hypervisor-based virtual network and between the hypervisor and virtual machines.
04. **Distributed IDS (DIDS),** consists of several IDSs, HIDS and NIDS, placed across a large network.

7.2 ISOLATION

Isolation helps to protect the virtual machines significantly from the inside, such as:

- Allows multiple users to co-habit the physical host but not attempting to any data leakage between users.
- Maybe some user obtains administration privileges. Isolation defenses the attacks to take over the shared resources.
- Isolation allows implementing mediation and monitoring process to analyze requests which are assigned to virtual machines.

7.3 DOS AND DDOS ATTACK MITIGATION

Defending a cloud interface against DoS and DDoS attack is difficult. But some techniques could be applied to mitigate the vulnerabilities. Some steps can be followed, such as: [75]

- Detect the attack as quickly as possible and determine the impact and the level of significance.
- Should try to mitigate the effects of the attack as much as possible.
- If the mitigation is not possible or the resources are not enough to mitigate the attack, then should migrate the virtual machine under attack to safe physical servers.
- To prevent such attacks, the allocated resource among user must be limited to bare a minimum.
- To eliminate the attacks, an efficient solution would be to dynamically use the scalability of cloud infrastructure to maintain availability.

Some defense strategies/ techniques can be taken to prevent/ mitigate DoS or DDoS attack:

- Virtual Machine Monitor
- Intrusion Detection System (IDS)
- Clusterized Firewall

- Detection and Cloud filter
- Limitation and Traceback
- **Statistical machine learning** (it supports a vector machine technique, which warn the system administrators and data owners of the type of attack and suggested possible actions to take.)
- **Hybrid Firewalling Architecture** [75]
    - It is a combination of physical and virtual cloud-based firewalling services.
    - The physical firewalls belong to the IT-Security infrastructure and the virtual firewalls reside on virtual machines.
    - The virtual firewalls can execute several operations such as analysis, monitoring and reporting.

7.4 SYN FLOOD ATTACKS AND SMURF ATTACKS MITIGATION

Some possible countermeasures for SYN flood attacks are:

1. Check periodically incomplete requests and randomly clear the incomplete connections. This can reduce the possibility of successful SYN attack.
2. Avoid allocating large memory for first packet, it is considered one of the best countermeasures.
3. Using of proxy server can be also reduce the SYN attack.
4. Circuit level firewalls can monitor the handshake of each new connection.
5. Increasing size of connections table can sometimes prevent the SYN flood attack.

The following steps can lead to a smurf attack:

1. Smurf attack constructs a spoofed packet including its source address and set it to real IP address of the victim.
2. A large amount of ICMP echo requests sends to the victim.
3. The victim receives the requests and then responds to the spoofed address.
4. It can build large amount of traffic on the side of victim's network and resulting in wreck of bandwidth which can crash the victim's server.

A smurf attack can be avoided by disabling IP broadcasting addresses at each network and firewall. [42] The routers can be configured in a way to ensure that the packets are not forwarded which is directed to broadcast addresses.

7.5 MEASURE TO PREVENT ACCOUNT HIJACKING

Record Hijacking is usually seen by the clients of the distributed computing system. Even though the cloud suppliers take at most activity and consideration in such manner [76] [77], yet the attackers discover their way in hijacking the client account. Beneath said are a couple of proactive estimates that can be taken in averting presentation to the security dangers caused by hijackers:

a. Setting up a convention that gives sharing record certifications between representatives or administrations.

b. Utilizing a solid two-factor confirmation strategy and track worker utilization of the stage for unapproved action.

c. Using a protected encryption administration framework, for example, that offered by venfi, ought to likewise be organized and grown particularly for use with a cloud stage.

d. In high private information stockpiling, disallow the sharing of record qualifications among clients and administrations.

e. Use solid two-factor validation methods are conceivable.

f. Utilize proactive checking to identify unapproved movement.

g. Understanding cloud supplier security approaches and SLAs, before singing in a cloud arrange.

These measures can diminish the introduction of customer account points of interest and information spillage to malignant insiders or outside programmer dangers. Associations

ought to know about these methods and in addition, normal guard top to bottom assurance systems to contain the harm that can be cause by this type of attack.

7.6 MALICIOUS INSIDER: MITIGATION TECHNIQUES

For successful mitigation of malicious insider attack adequate protective measures should be implemented on both cloud providers and client side.

Client side:

I. Confidentiality:

Confidentiality is big issue in safeguarding data in cloud platform. Even in lass, where the company use most of the cloud infrastructure. Yet the cloud user could not detect that someone else has gain access to their company data. Using OS level security mechanism. The cause behind that, if someone who works for the cloud itself has access to physical infrastructure which users could not control.

To solve this problem partially the users could implement cryptographic techniques to safeguard their data. It is a practical solution mainly implemented for bulk storage of data. [78]

II. Availability:

Availability is another very important issue in case of malicious insider's attack. Ideally to be protected from suck harmful attacks the cloud providers should allocate their data in different geographical locations with automatic switching to the backup data centers.

In case the primary data centers fails, such measures can work if the malicious insider could not interfere with multiple data centers at the same time.

Providers Side:

From the side of the cloud service providers quite a few detection and mitigation techniques could be implemented.

III. Separation of Duties:

Strict separation of duties for the cloud service providers employees especially the power users like System administrators, is one of the key tasks to protect such insider attacks. The insider will have limited access to the infrastructure and the only way he/she can attempt to obtain restricted access but by doing so can be detected. [78]

IV. Logging:

All the user actions, especially the action of the power users like system administrator, must be heavily logged and audited. Apart from detecting potential insider attack, kit can also be used to detect continuous action checking way.

CHAPTER 08: A FINAL WORD

8.1 CONCLUSION

Cloud computing has several service models and deployment models to utilize rapid and virtualized technology completely. As it has become one of the fastest growing fields in information technology also, it has to face the new security issues on a regular basis besides. Denial-of-service (DoS), as well as, distributed denial-of-service is one of the most security threat for a cloud environment. For an example, using a cloud environment, a hacker can launch a huge number of ACK/ SYN packets on a targeted IP or server to make the resource unavailable or down. The same issue can be performed from another side to make a cloud server or service unavailable or inaccessible.

In this paper as well as the project, we have tried to analyze the attack techniques and find out the number of vulnerabilities related to a cloud environment. We have tried to perform some of the techniques inside our personal lab to measure the effect of such kind of vulnerabilities. The future work related to cloud computing will give us enough opportunity to learn and perform more about cloud security and its vulnerabilities.

8.2 LIMITATION AND DRAWBACKS

8.2.1 Working Environment

Cloud Environment

As a part of our project our experiment was based on cloud environment. We intended to pursue our research on ‘FH private cloud’ but unfortunately, we were unable to utilize it because the cloud server was offline during our project. We would have better idea regarding to the cloud computing if we got access on ‘FH Cloud’. We were somehow managed to work on our local/ virtual environment.

Virtual Environment

We created a virtual environment using the software 'Virtual Box'. We have installed our attacker computer and victim computer into it. Though it is not a real environment, so we were not completely successful to deploy our tests.

Local Network Environment

Though we were testing on our local network, so we cannot examine further techniques in the real world. In our dataset, we have only our local IP address because all techniques were performed at the local environment. However, attacking outside of the local area is illegal and risky.

8.2.2 Attacking Tools

LOIC anonymity Issue:

Low orbit ion canon (LOIC) does not take any attempt to hide the identity of the user or an attacker. Attackers using the LOIC are easy to detect as the IP addresses are visible to the victim system. Along with the sending packets LOIC sends the attacker IP address as well, or in other way the attackers IP address is included in the packets that is sent to the victim. Moreover, Internet service providers can easily identify the attackers IP address.

Pentmenu bash script is a powerful tool to perform a DoS attack but only implemented and tested on Debian and Arch. Therefore, to perform a DoS attack using pentmenu the attacker must have Debian based Linux distributions. [83] Unfortunately, this script cannot be used from Windows or apple platform.

8.2.3 Data Visualization

1. The dataset we retrieve from Wireshark contains a huge sum of data, for our effective analysis and visualization we use a fraction of the data.

2. When we convert our raw data to CSV format some undesired fields add up to our data, but they don't have any effect on our final output but to get rid of it had to spend some time.

8.3 FUTURE WORK

Cloud computing is a large area to study, understand and learn. On the other hand, attack techniques are also more difficult to understand and examine. Moreover, new attack techniques are being introduced regularly. As a first step of the future work we will research more to find out the limitations of our current work. Besides, develop new ideas and find suitable parameters to analyze the attack techniques inside our own lab. Find out the mitigating techniques to secure the resources from internal or external vulnerability threats will be a part of future work. Our current work was limited to local network, so we would try to make a virtual web server, so that, we could examine vulnerabilities outside of the local network. Furthermore, we have the interest to analyze and work with websites and web applications to extend our knowledge regarding web technologies.

WORK MATRIX

Work / Student		Arifur	Adnan	Saiful
Project Idea		✕	✕	✕
Project work framework		✕	✕	✕
Project documentation framework				✕
Report Writing	Project Abstract			✕
	Chapter 01			✕
	Chapter 02	✕	✕	✕
	Chapter 03	✕		✕
	Chapter 04	✕		✕
	Chapter 05	✕	✕	
	Chapter 06, 07, 08	✕	✕	✕
Literature review		✕		✕
Scenario setup and Network configuration		✕		
Work with attacking tools		✕		✕
Collect work data		✕	✕	✕
Analyzing data after vulnerabilities affect		✕	✕	
Visualization of All attacks data			✕	

REFERENCES

01. Dr. Daniel Fallman; ‘Ubiquitous Computing’, page [12-13]
02. https://csrc.nist.gov/Projects/Cloud-Computing
03. NIST Cloud Computing Standard Roadmap; page 14
04. https://www.techopedia.com/definition/14469/measured-service-cloud-computing
05. K., "The Internet of Things: A survey," Computer Networks, vol. 54, pp.2787-2805, 2010.
06. https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT
07. Harbor Research, “What Exactly Is The "Internet of Things?”, March, 2014.
08. L Liang, K Zheng, Q Sheng, X Huang; A Denial of Service Attack Method for an IoT System
09. M Grabovica, D Pezer, S Popic, V Knezevic; Provided security measures of enabling technologies in Internet of Things (IoT): A survey
10. Y Haoyu; “WIFI technology and development”, Silicon Valley,(2010)
11. M Denis, C Zena, T Hayajneh; Penetration Testing: Concepts, Attack Methods, and Defense Strategies.
12. https://www.techopedia.com/definition/24748/cyberattack
13. Cyber Security, a Threat to Cyber Banking in South Africa; By Thierry Mbah Mbelli and Barry Dwolatzky
14. Data Breach on the Critical Information Infrastructures: Lessons from the Wikileaks; By Azmi, Zulhuda and Jarot; page-307
15. https://sg.channelasia.tech/article/644115/singapore-suffers-largest-data-breach-country-history-1-5m-affected/
16. https://sg.channelasia.tech/article/646384/data-breach-hits-british-airways-380-000-payments-affected/
17. Understanding virtualization, https://www.redhat.com/en/topics/virtualization
18. Importance and applications of virtualization, https://www.networkworld.com /article/3234795/virtualization/what-is-virtualization-definition-virtual-machine-hypervisor.html
19. Definition of Virtualization, https://www.vmware.com/solutions/virtualization.html
20. Types of Hypervisor, https://opensource.com/resources/virtualization
21. Virtual machine, https://searchservervirtualization.techtarget.com/definition/virtual-machine
22. https://geek-university.com/ccna-security/confidentiality-integrity-and-availability-cia-triad/
23. X Meng, J Shi, X Liu, H Liu, L Wang; Legacy Application Migration to Cloud
24. https://open.blogs.nytimes.com/2008/05/21/the-new-york-times-archives-amazon-web-services-timesmachine/
25. https://timesmachine.nytimes.com/timesmachine/1942/10/04/issue.html
26. https://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS
27. NIST Special Publication 800-145; https://csrc.nist.gov/publications/detail/sp/800-145/final

28. G Liu; Research on Independent SaaS Platform
29. https://www.webopedia.com/TERM/E/everything-as-a-service_xaas.html
30. Study on TCP/IP Protocol Suite, https://study-ccna.com/tcpip-suite-of-protocols/
31. DoS attacks Defn, https://www.techopedia.com/definition/24841/denial-of-service-attack-dos
32. DoS attacks that made headlines, https://www.csoonline.com/article/3226399/security/6-dos-attacks-that-made-headlines.html
33. Analysing the Origins of a DDoS Attack, https://blog.sucuri.net/2014/05/map-of-a-ddos-attack.html
34. Botnet assisted ddos attacks, https://thecybersecurityplace.com/statistics-on-botnet-assisted-ddos-attacks-in-q1-2015/
35. https://securelist.com/ddos-attacks-in-q4-2016/77412/
36. Types of DDoS attacks, https://www.esecurityplanet.com/network-security/types-of-ddos-attacks.html
37. DDoS attacks, https://www.incapsula.com/ddos/ddos-attacks.html
38. T.Siva, E.S.Phalguna Krishna, Controlling various network based ADoS Attacks in cloud computing environment: By Using Port Hopping Technique, International Journal of Engineering Trends and Technology (IJETT), vol. 4, May 2013.
39. https://www.incapsula.com/ddos/attack-glossary/syn-flood.html
40. B. Prabadevi, N.Jeyanthi, Distributed Denial of service Attacks and its effects on Cloud Environment-a Survey, IEEE Explore, 2014.
41. S.S. Chopade, K.U. Pandey, D.S. Bhade, Securing Cloud Servers against Flooding Based DDOS Attacks, in Proc. International Conference on Communication Systems and Network Technologies,2013.
42. Smurf Attack, https://www.cloudflare.com/learning/ddos/smurf-ddos-attack/
43. Slowloris attack, https://witestlab.poly.edu/blog/slowloris/
44. https://www.semanticscholar.org/paper/Towards-a-Stochastic-Model-for-Integrated-detection-Mir-Kim/a77369202e76e0f4325c2142ea3f059800499e6c
45. Amazon Web Services: Overview of Security Processesaws_blog/AWS_Security_Whitepaper2008_09.pdf.
46. Amazon uses HackAlert™ - http://malwareinfocom/ mal_faq_hackalert.html
47. T. Moore and R. Clayton, “Examining the impact of website take-down on phishing”, In Anti- Phishing Working Group eCrime Researcher’s Processeslaws_blog/AWS_Security_Whitepaper Summit (APWG eCrime), pp. 1–13, ACM Press, New York, 2007.
48. Christina A. Annie., “Proactive measures on account hijacking in cloud computing network”, Asian Journal of Computer Science and Technology, ISSN 2249-07-01, Vol. 04
49. Jøsang, A., & Pope, S. (2005). User Centric Identity Management. AusCERT Asia Pacific Information Technology Security Conference. Brisbane, Australia: AusCERT.

50. Günsberg, W. A. (2009). Federated Identity Management: The auditor's perspective. Master Thesis, VU University Amsterdam, Amsterdam.
51. Bi, L. (2008). Identity and access: How to protect your business. Journal of Corporate Accounting & Finance, 19 (5), 9-13.
52. Hermans, J., & ter Hart, J. (2005). Identity & Access Management: operational excellence of 'in control'? Compact Magazine, 2005 (3), pp. 47-53.
53. Mather, T., Kumaraswamy, S., & Latif, S. (2009). Cloud Security and Privacy: An Enterprise Perspective on Risk and Compliance. Sebastopol, United States of America: O'Reilly Media, Inc.
54. Jansen, W., & Grance, T. (2011). Guidelines on Security and Privacy in Public Cloud Computing. Information Technology Laboratory. Gaithersburg, United States of America: National Institute of Standards and Technology.
55. Sturrus E., (2009). Identity and Access Management in a Cloud Computing Environment, Erasmus School of Economics.
56. Jadhav S., "A Survey on Safe Information Sharing and Query Processing Via Organization of Cloud Computing", International Journal of Science and Research (IJSR), ISSN (Online): 2319-7064.
57. Armbrust M., Fox A., Griffith R., Joseph A., Katz R., Konwinski A., Lee G., Patterson D., Rabkin A., Stoica I., Zaharia M., "Above the Clouds: A Berkeley View of Cloud Computing", UCB/EECS-2009-28, Univ. of California at Berkley, USA, 2009.
58. Kandias M., Mylonas A., Theoharidou M., Gritzalis D., "Exploitation of auctions for outsourcing security-critical projects", In: Proc. of the 16th IEEE Symposium on Computers and Communications (ISCC '11), Greece, 2011.
59. Johnson, C., "CyberSafety: On the Interactions between Cyber Security and the Software Engineering of Safety-Critical Systems".
60. Mather, T., Kumaraswamy, S., Latif, S., "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice)", O'Reilly Media, USA, 2009.
61. Theoharidou M., Kotzanikolaou P., Gritzalis D., "Towards a Criticality Analysis Methodology: Redefining Risk Analysis for Critical Infrastructure Protection", in Proc. of the 3rd IFIP International Conference on Critical Infrastructure Protection (CIP-2009), Springer, USA, March 2009.
62. Theoharidou M., Kokolakis S., Karyda M., Kiountouzis E., "The insider threat to Information Systems and the effectiveness of ISO 17799", Computers & Security, Vol. 24, No. 6, pp. 472-484, 2005.
63. Bishop M., Gates C., "Defining the Insider Threat", in Proc. of the 4th Annual Workshop on Cyber Security and Information Intelligence Research, Tennessee, Vol. 288, 2008.
64. Shaw E., Ruby K., Post J., "The insider threat to information systems: The psychology of the dangerous insider", Security Awareness Bulletin, Vol. 2, pp. 1-10, 1988.
65. Kandias M., Virvilis N., Gritzalis D., "The Insider Threat in Cloud Computing", Athens University of Economics and Business, Greece.

66. Botnet assisted ddos attacks, https://thecybersecurityplace.com/statistics-on-botnet-assisted-ddos-attacks-in-q1-2015/
67. https://www.aircrack-ng.org/doku.php?id=airodump-ng
68. GinjaChris pentmenu, https://github.com/GinjaChris/pentmenu
69. “LOIC Will Tear Us Apart” The Impact of Tool Design and Media Portrayals in the Success of Activist DDOS Attacks, Article in American Behavioral Scientist 57(7):983-1007 · July 2013.
70. LionSec Xerosploit, https://github.com/LionSec/xerosploit
71. Paolo Farina, Enrico Cambiaso, Gianluca Papaleo, Maurizio Aiello, "Understanding DDoS Attacks from Mobile Devices", IEEE 2015 3rd International Conference on Future Internet of Things and Cloud
72. Sabari Giri Murugan, Ganesan, Thiyagu, "Detecting & Isolating Anonymous Nodes Using Honeypot in Networks". International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 3, 2018.
73. Websploit Package Description, https://tools.kali.org/web-applications/websploit
74. A Carlin, M Hammoudeh, O Aldabbas: Defence for Distributed Denial of Service Attacks in Cloud Computing
75. Adrien Bonguet and Martine Bellaiche; A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing
76. “Cloud Computing - Benefits, risks and recommendations for information security”, November 09 ByENISA.
77. Christina A. Annie., “Proactive measures on account hijacking in cloud computing network”, Asian Journal of Computer Science and Technology, ISSN 2249-07-01, Vol. 04
78. Kandias M., Virvilis N., Gritzalis D., “The Insider Threat in Cloud Computing”, Athens University of Economics and Business, Greece.
79. https://blogs.technet.microsoft.com/chenley/2011/02/09/hypervisors/
80. Introduction to the Best Free DOS Attacking Tools, https://resources.infosecinstitute.com/dos-attacks-free-dos-attacking-tools/
81. DoS attack using Kali, https://www.crackitdown.com/2018/04/how-to-do-ddos-attack-using-kali-linux.html
82. Xerosploit toolkit, https://gbhackers.com/kali-linux-tutorial-xerosploit/
83. Pentmenu, https://github.com/GinjaChris/pentmenu