CLOUD-BASED DDoS ATTACK AND POSSIBLE COUNTERMEASURES

[1]Tulsiyani Archana, [2] Chandresh Parekha
[1] Student M. Tech Cyber Security, [2]Assistant Professor
[1] Department of IT & Telecommunication
[1] Raksha Shakti University, Ahmedabad, Gujarat, India

Abstract: In the aeon of the internet, storing your files and important document in the traditional environment which used limited space to store was starting to become inconvenient. The availability of document is becoming prime priority. So, the concept of storing data on the cloud came into view. As the time passed the cloud was further divided into public, private and hybrid to fulfil different purposes. Distributed denial of service (DDoS) attack is one of the attacks, which has an immense danger to the availability of the internet. Cloud has many securities promoting among which DDoS attacks have prime priority. Cloud Security matter being premier for the private enterprises, the denial of service attacks is rated as the highest priority threat. One of the huge problem is to find the details of attack as many organization hold off to revel that they were attack due to the panic of the scandal. It exhausts victim's bandwidth. In this paper an overview of distributed-denial-of-service, different types of attack, different types of techniques, and their countermeasures.

***Index Terms* - Avaibility, Attack, DDoS, Security.**

I. INTRODUCTION

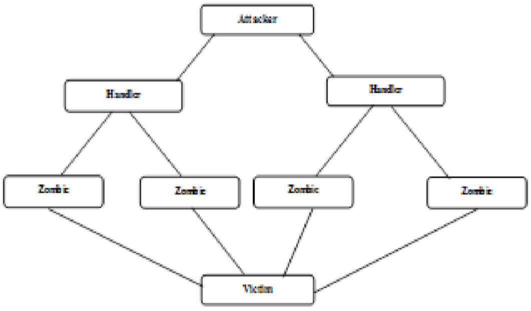
Cloud Computing is a strong candidate for IT implementations because it provides cost-effective and pay-as-you-go based access to on-demand computer functions and services. Many companies are moving their IT structure to the cloud. Infrastructure clouds have many advantages over fixed infrastructure. These benefits include "pay-as-you-go", availability of data when needed and much more. The literature discusses various issues that are discussed in the literature [4], [5]. The "availability" means that the information should be accessible at all times. The threat to Internet availability is a major issue that is ahead of the game in promoting the growth and survival of e-business and other products. Internet is susceptible to errors like another product. Internet outages can be random or deliberate. The design of the Internet focuses mainly on the provision of functionality. Therefore, it offers little attention in designing damage control due to random errors. On the other hand, eloquent attacks by the malicious insider / hacker / cracker have no answer to the original design of the Internet. Security issues associated with cloud computing are applicable to different subscribers to enable informed cloud adoption. In addition to data breaches, the cyber security community often visits the attack room for cloud-related solutions, as these issues impact budget, resource management, and service quality. A Denial of Service (DoS) attack prevents legitimate users from purchasing the services. DDoS does this by sending a lot of information that causes a crash. Some common DDoS attacks are SYN-ATTACK, TEARDROP, SMURF, FINGER BOMB, BLACK HOLE, and so on. Distributed Denial-of-Service (DDoS) attacks worsen or completely disable services for legitimate users by providing communication and / or computational resources of the target. DDoS attacks are an escalated form of DoS attack in which attacker's target hundreds or even thousands of compromised hosts known as zombies against a single target. These zombie hosts are unknowingly recruited by the millions of unprotected computers that access the Internet over high-bandwidth connections and always-on connections. There are five types of DOS attacks mentioned. When attacking at the network level, the target device is on the network.

Application-level attacks identify errors or vulnerabilities in the application to exploit them for DOS attacks. A port scan to identify open ports of a remote application is very common in this perspective. In a plan where most other attacks are now identified, application-level attacks offer attackers a higher rate of success [6].For example, the source IP address of a data packet.

There are different types of DDoS attacks like in[1][2]. The most common form of DDoS attack is called packet flooding attack, where a large number of supposedly legitimate TCP, User Datagram Protocol (UDP), or Internet Control Message Protocol (ICMP) packets are routed to one specified destinations. According to Peng [3], defending against this type of attack is not easy for two reasons. First, the number of bots involved in a DDoS attack in large topographical area. The amount of traffic sent by individual zombies could be inundated. Second, zombies usually mislead their IPs under the attacker's control, making it very difficult to trace even the zombies. [23].

II. OVERVIEW OF DDOS

The operating system and network protocol are not developed by focusing on security, which in effect provides the number of unpatched and unsecured machines on the Internet that hackers use to perform their activities. These unsecured and unpatched machines are used as a major source of the DDoS attacker as their army of bots / zombies to attack. These bots / zombies are vulnerabilities for the public network because hackers can attack these types of systems and inject the malicious code or use other techniques to control those types of machines and then add them to the army of their bots / zombies. These evil machines can be in hundreds or thousands of numbers. They all behave like an attacker's agent. The network of this type of malicious machine is called a "zombie network". The size of the zombie determines the strength of the attack. For example, if the number of zombies / bots is large, then the impact of the attack is severe. The following figure 3 shows how the DDoS attack works. In the "botnet" or "zombie network" you choose the "HANDLER" who controls and controls the bots. The bots attack directly to the victim. Under each "handler" there is a group of agents (bots). These "handlers" are the medium of communication between "Bots" & "Master". It also hands over the information of the victim received from the "Bots". Since "handler" and the "zombie" are also malicious machines in the public network under the control of an attacker, the users of these machines are not even aware that they are used as part of the botnet network. A typical plan of the DDoS attack is mentioned below [23].



Architecture of DDoS

III. CLASSIFICATION OF DDOS

DDoS Attacks is considered one of the biggest attacks causing chaos both in the network and in applications. For better understanding and development of various tools, DDoS attacks have been classified into 3 types:

3.1 Volume Based Attacks:

Considered one of the most commonly used attack techniques for launching DDoS attacks. The main mode of volume-based attacks is to saturate the bandwidth of the victim's website or network by using various techniques. This prohibits legitimate users from accessing the site or the network, rendering the services unusable to users. Leads to server crash. The main techniques used to start disk-based attacks are UDP floods, ICMP floods, and other spoofed attack floods. The magnitude of volume-based attacks is measured in bits per second. In 2016, it was observed that there were about 650 Gbps DDoS floods in excess of 150 million packets per second (Mpps).

3.2 Protocol-Based Attacks:

Protocol-based attacks consume server resources These attacks are mainly focused on the exploits of Layer 3 and 4 vulnerabilities in the OSI model. The scale of protocol-based attacks is measured in packets per second (Pps). They are also referred to as state exhaustion attacks. Some of the common attacks are SYN Floods, fragmented packet attacks, Ping of Death, Smurf DDoS. [23]

3.3 Application Based Attacks:

Application based attacks are generally considered as most devastating as it is rather harder to identify a DDoS attacks is happening. Also known as Layer 7 DDoS attack. A single HTTP request is cheap to execute on the client side and can be expensive for the target server to respond to as the server often must load multiple files and run database queries in order to create a web page. Types of Application based attacks are Http flood attacks, xml-based attacks. Attack traffic is usually legitimate, targeting the application layer and involves triggering a back-end process that hogs the resources and making it unavailable. For this reason, these types of attacks are comparatively harder to mitigate. The number of attacks in Q4 reached an all-time high, with an average of 889 application layer assaults per week.

IV. EXISTING SYSTEM

A different tools or "stressors" are available for free on the internet. The use of these tools is considered legal because researchers occasionally run stress tests against their networks to understand the damage that has been done after an actual attack. Some attack tools are specialized and focus only on a specific area of a particular layer of the protocol stack. Others, however, are designed so that multiple attack vectors can simultaneously target multiple levels. These tools can be roughly divided into several groups:

Low and slow attack tools As the name defines, it both use a small amount of data and work very slowly. These tools are programmed to send little amounts of data across multiple connections to keep ports open on a target server as long as possible. These tools continue
to use server resources until a destination server can't sustain additional connections. Slow attacks can few times be effective, even if they don't use a distributed system like a botnet and are typically used by a single computer.

Protocols and Transport Layer (L3 / L4) attack tools If you use the tools below, these tools use protocols such as UDP to send huge amounts of data to a destination server. While these attacks are often less effective, they are typically found in the form of DDoS attacks, where the advantage of additional attacking machines adds to the effect. Some commonly used tools are:

Low Orbit Ion Cannon (LOIC) The LOIC is an open-source application which tests the stress. It enables both TCP and UDP protocol layer attacks with a user-friendly WYSIWYG interface. Due to the popularity of the original tool, derivatives have been developed that can be used to launch attacks. [23]

High Orbit Ion Cannon (HOIC)

This tool was created to replace the LOIC by extending its capabilities. By using the HTTP protocol, the HOIC is able to launch targeted attacks that are difficult to mitigate. [23]

Slowloris

Slowloris is an application that triggers a slow attack on a targeted server. The elegance of Slowloris is the limited amount of resources it takes to create a harmful effect. [23]

V. PROPOSED METHOD

TOOLS USED

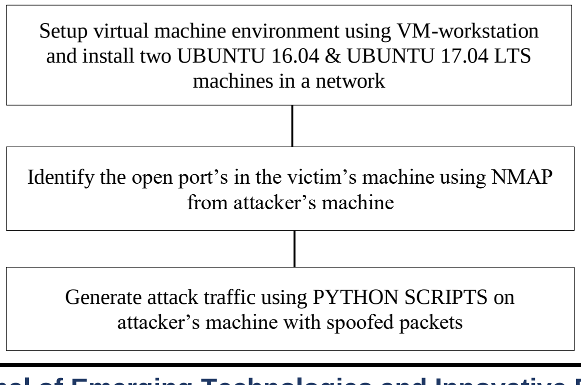
Snort: Snort is an open source arrange interruption aversion framework that can perform constant movement examination and parcel signing in IP systems. It can perform log examination, content pursuit/coordinating, and can be utilized to recognize an assortment of assaults and tests, such as, cradle floods, port sweeps, CGI assaults, and then some. [18]

N-MAP ("Network Mapper"): NMAP is a uninhibitedly accessible system investigation instrument. NMAP is utilized to perform port checking, working framework identification and host recognition, et cetera. [19]

PYTHON: Python is a translated, question situated abnormal state programming dialect with dynamic semantics. Python's straightforward, simple to-learn language structure accentuates coherence and accordingly diminishes the cost of program upkeep. Python bolsters modules and bundles, which advances measured quality of the program and reuse of code.

IP TABLES: IP Tables is a present Linux firewall component and successor to ipfilter and ipchains. The fundamental reason for existing is bundle sifting in light of header fields, e.g. IP locations, TCP and UDP ports, and TCP banners. Initially the most famous firewall/NAT bundle on Linux was ipchains, yet it had various inadequacies. To settle this, the net filtering association chose to make another item called iptables.

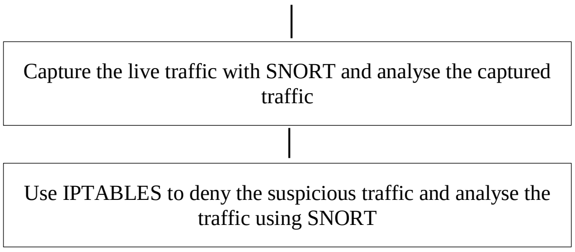
STEPS OF IMPLEMENTAION:



Setup virtual machine environment using VM-workstation and install two UBUNTU 16.04 & UBUNTU 17.04 LTS machines in a network

Identify the open port's in the victim's machine using NMAP from attacker's machine

Generate attack traffic using PYTHON SCRIPTS on attacker's machine with spoofed packets



Capture the live traffic with SNORT and analyse the captured traffic

Use IPTABLES to deny the suspicious traffic and analyse the traffic using SNORT

Implementation Steps

Step1: To set up an isolate organize utilizing virtualization. VMware Workstation is utilized to set up an isolate system and two UBUNTU 16.04 LTS and UBUNTU 17.04 working frameworks are introduced on it.

Step2: Identify open ports on casualty machine by utilizing NMAP instrument. On the off chance that we run Python content on casualty machine, at that point NMAP recognizes the port identified with running of customer server program on casualty machine.

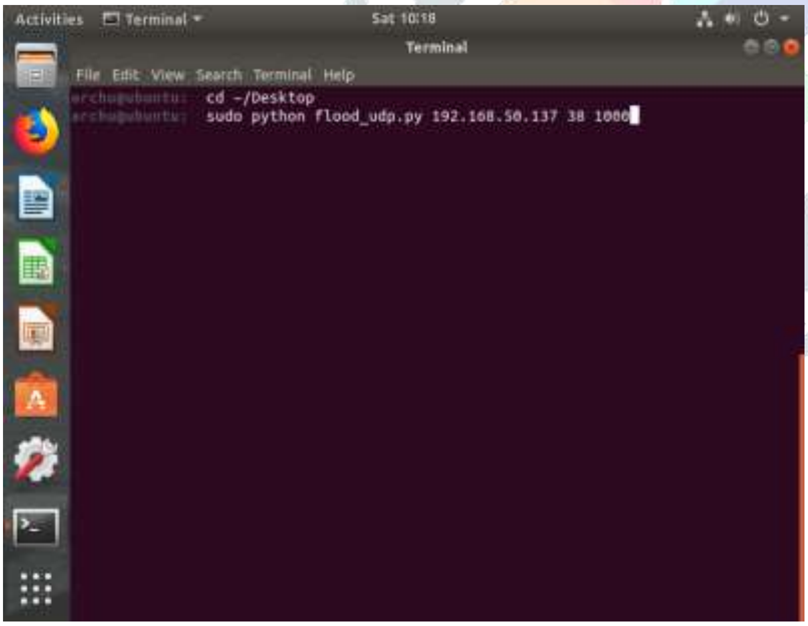
Step3: Run the IP table administer on assailant machine with the end goal that casualty's bit's don't get RSTs.

Step4: Run Snort device on casualty's machine keeping in mind the end goal to identify and examine DDoS assault.

Step5: Use IP tables to square SYN surge assaults on casualty's machine.

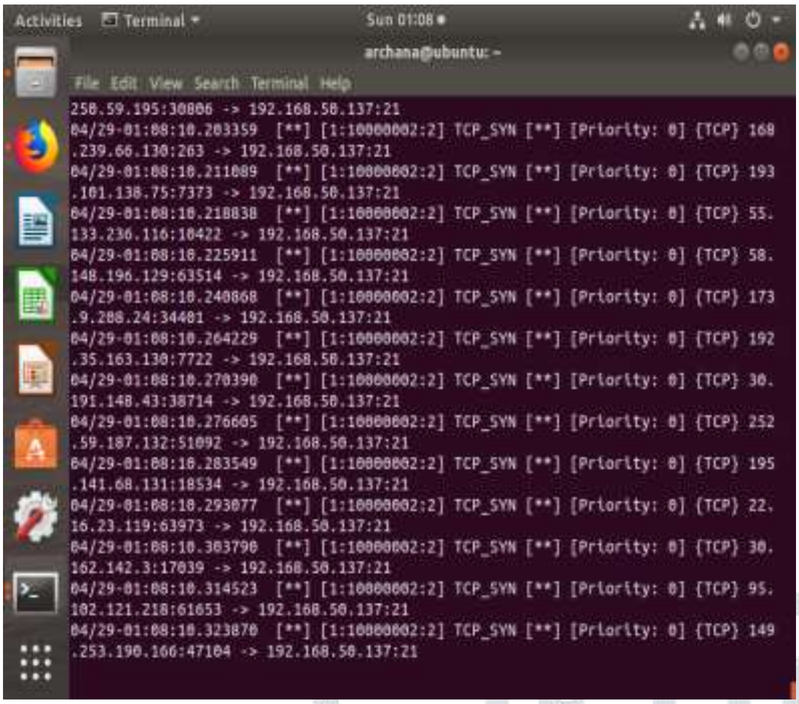
Step6: After blocking movement utilizing IP tables again catching and examining of live activity utilizing grunt. The over six stages are executed according to outline appeared in Fig2.

VI. EXPERIMENTAL RESULTS



```
archu@ubuntu:  cd ~/Desktop
archu@ubuntu:  sudo python flood_udp.py 192.168.50.137 38 1000
```

Udp flood attack



```
250.59.195:30806 -> 192.168.50.137:21
04/29-01:08:10.203359  [**] [1:10000002:2] TCP_SYN [**] [Priority: 0] {TCP} 168
.239.66.130:263 -> 192.168.50.137:21
04/29-01:08:10.211089  [**] [1:10000002:2] TCP_SYN [**] [Priority: 0] {TCP} 193
.101.138.75:7373 -> 192.168.50.137:21
04/29-01:08:10.218838  [**] [1:10000002:2] TCP_SYN [**] [Priority: 0] {TCP} 55.
133.236.116:10422 -> 192.168.50.137:21
04/29-01:08:10.225911  [**] [1:10000002:2] TCP_SYN [**] [Priority: 0] {TCP} 58.
148.196.129:63514 -> 192.168.50.137:21
04/29-01:08:10.240868  [**] [1:10000002:2] TCP_SYN [**] [Priority: 0] {TCP} 173
.9.208.24:34401 -> 192.168.50.137:21
04/29-01:08:10.264229  [**] [1:10000002:2] TCP_SYN [**] [Priority: 0] {TCP} 192
.35.163.130:7722 -> 192.168.50.137:21
04/29-01:08:10.270390  [**] [1:10000002:2] TCP_SYN [**] [Priority: 0] {TCP} 30.
191.148.43:38714 -> 192.168.50.137:21
04/29-01:08:10.276605  [**] [1:10000002:2] TCP_SYN [**] [Priority: 0] {TCP} 252
.59.187.132:51092 -> 192.168.50.137:21
04/29-01:08:10.283549  [**] [1:10000002:2] TCP_SYN [**] [Priority: 0] {TCP} 195
.141.68.131:18534 -> 192.168.50.137:21
04/29-01:08:10.293077  [**] [1:10000002:2] TCP_SYN [**] [Priority: 0] {TCP} 22.
16.23.119:63973 -> 192.168.50.137:21
04/29-01:08:10.303790  [**] [1:10000002:2] TCP_SYN [**] [Priority: 0] {TCP} 30.
162.142.3:17039 -> 192.168.50.137:21
04/29-01:08:10.314523  [**] [1:10000002:2] TCP_SYN [**] [Priority: 0] {TCP} 95.
102.121.218:61653 -> 192.168.50.137:21
04/29-01:08:10.323870  [**] [1:10000002:2] TCP_SYN [**] [Priority: 0] {TCP} 149
.253.190.166:47104 -> 192.168.50.137:21
```

TCP Flood detection using snort

VII. FUTURE WORK

DDoS Attack tools are available plenty in the market, which are generally open-source and can be used with few efforts. But the same is not true with the detection & prevention tool. DDoS attack prevention tools or software are too costly to be implemented by small vendors, business or educational institutes. So, the future proposed work consists of a tool that is easily available & used by the small corporate business and educational institutes that helps to mitigate the deadliest DDoS attack.

VIII. CONCLUSION

In this paper, we presented a review of Distributed-Denial-of-service-attack along with the possible countermeasures in cloud environment. Attacks based on Network layer are reviewed. In this we have tried to give the insight of the DDoS Attack by including the Overview of DDoS, Classification, Motivation of DDoS Attacks, its problem along with the recent DDoS incidents and the implementation steps of counter measures are presented.

IX. REFERENCES

[1]. Douligeris C.and Mitrokotsa A.,"DDoS Attacks and Defense Mechanisms: Classification and State of the Art," Computer Journal Of Networks,vol.44,no.5,pp.643-666,2004.

[2]. Mirkovic J.and Reiher P.,"A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," Computer Journal of ACM SIGCOMM,vol.34,no.2,pp.39-53,2004.

[3]. Peng T.,Leckie C.,and Ramamohanarao K.,"Survey of Network Based Defense Mechanisms Countering the DoS and DDoS Problems,"Computer Journal of ACM Computing Surveys,vol.39,no.1,pp.123-128,2007.

[4]. B.R.Kandukuri,V.R.Paturi,A.Rakshit,Cloud security issues,in: Services Computing,2009.SCC '09.IEEE International Conference on,2009,pp.517–520,doi: 10.1109/SCC.2009.84 .

[5]. L.M.Kaufman,can public-cloud security meet its unique challenges? IEEE Se-cur Priv 4 (8)(2010)55–57.

[6]. Nilesh A.Suryawanshi S.R.Todmal DDoS Attacks Detection of Application Layer for Web Services using Information based Metrics International Journal of Computer Applications (0975-8887)Volume 117-No.9,May 2015

[7]. Gaurav Somania,M.S.(30 march 2017).DDoS Attacks in Cloud Computing: Issues,Taxonomy,and Future Directions. Elsevier,19.

[8]. Gibson S.,"The Strange Tale of the Denial of Service Attacks Against GRC.COM," http://grc.com/dos/grcdos.htm,2007.

[9]. Monica Sachdeva,Gurvinder Singh,Krishna Kumar and Kuldip Singh," DDoS Incidents and their Impact: A Review",The International Arab Journal of Information Technology,Vol.7,No.1,January 2010

[10]. Howard J.,"An Analysis of Security Incidents on the Internet," PhD Dissertation,Carnegie Mellon University,1997 Statics

[11]. K.Santhi Sri,PRSM Lakshmi," DDoS Attacks,Detection Parameters and Mitigation in Cloud Environment",International Journal for Modern Trends in Science and Technology,Volume: 03,Special Issue No: 01,February 2017

[12]. http://www.bcmpedia.org/wiki/Denial_of_Service

[13]. https://www.us-cert.gov/ncas/tips/ST04-015

[14]. www.incapsula.com/blog/650gbps-DDoS-attack-leet-botnet.html

[15]. https://www.cloudflare.com/learning/DDoS/what-is-a-DDoS-attack

[16]. https://blog.thousandeyes.com/how-to-analyze-DDoS-attackf-dns-infrastructure

[17]. Adrien Bonguet and Martine Bellaiche A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defences in Cloud Computing future internet 2017.

[18]. https://www.snort.org/faq/what-is-snort

[19]. https://nmap.org/

[20]. https://docs.python.org/3/

[21]. https://help.ubuntu.com/community/IptablesHowTo

[22].D.DeepthiRani,T.V.SaiKrishna,G.Dayanand-am, Dr. T.V.RaoTCP Syn Flood Attack Detection And PreventionInternational Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue10 – Oct 2013

[23].Archana Tulsiyani, Ekta Singh, Asst. Prof. Chandresh ParekhaDDOS Attacks and Possible Countermeasures : A Review International Journal of Scientific Research in Computer Science, Engineering and Information Technology Volume 2 | Issue 6 | ISSN : 2456-3307