International Journal of Innovative Research in Science and Engineering
Vol. No.2, Issue 04, April 2016
www.ijirse.com
ISSN: 2454-9665

DISTRIBUTED DENIAL-OF-SERVICE

Er.Gajendra Singh[1], Er.Manoj Gupta[2]

[1,2]Asst.Prof., Department of Computer Science & Engineering ,

Vedant College of Engineering & Technology ,Bundi ,Rajasthan, (India)

ABSTRACT

Distributed Denial-of-Service (DDoS) is an increasingly worrying threat to availability of Internet resources. DDoS attacks have recently emerged as one of the most newsworthy, if not the greatestweaknesses of the Internet. The variety and number of both attack and defense approaches are overwhelming. Distributed denial-of-service (DDoS), is a relatively simple, yet very powerful technique to attack Internet resources. With little or no advance warning, a DDoS attack can abruptly drainthe computing and communication resources.

We here discuss DDoS in the current scenario, representing a detailed description of exactly how this attack works and why is it hard to cope. Also, various principles and challenges encountered in defense against DDoS are explained with the unvarying or habitual method of the attacks and its classification. Research issues in DDoS are highlighted and in the long term picture, an integrated approach to the DDoS problem is proposed that will bring this classic old problem under control, if not eliminate it entirely.

Thus a better understanding of the problem, current solution space and future scope are provided.

I. INTRODUCTION

General Idea: -

Distributed denial-of-service (DDoS), is a relatively simple, yet verypowerful technique to attack Internetresources. With little or no advance warning , a DDoSattack can abruptly drainthe computing and communication resources of its victim within a short time,until the attack is resolved or in some cases slowly eat up the resources without being noticed. Thus these disruptive or degrading attack flows often lead to complete shutdowns of Internet resources or at least cause performancedegradations.As per the recent survey conducted by FBI/CSI, these attacks are second most dreadful attacks in terms of revenue losses after information thefts. Even some of thelargest computer makers and the web-based service providersare not immune from this problem.

Definition: -

A Denial of Service (DoS) attack is an attack with the purpose of preventing legitimate users from using a specified network resource such as a website, web service, or computer system.

A Distributed Denial of Service (DDoS) attack is a coordinated attack on the availability of services of a given target system or network that is launched indirectly through many compromised computing systems. The services under attack are those of the “primary victim”, while the compromised systems used to launch the attack are often called the “secondary victims.”In February of 2000, one of the first major DDoS attacks was waged against Yahoo.com, keeping it off the Internet for about 2 hours, costing it lost advertising revenue.

International Journal of Innovative Research in Science and Engineering
Vol. No.2, Issue 04, April 2016
www.ijirse.com
ISSN: 2454-9665

II. OVERVIEW

As we have already discussed, Denial of Service (DoS) is the act of performing an attack which prevents the system fromproviding services to legitimate users. Denial of Service attacks takes many forms, and utilizes many attack vectors. When successful, the targeted host may stopproviding any service, provide limited services only or provide services to some users only.

Fig. 1. shown below depicts an idea how an attack is carried out by a Hacker/Attacker. A DDoS attacker implants attack programs in various machines (called Zombies) over the internet. These zombie machines under the control of handlers send attack packets whichconverge at victim/target or its network to exhaust either its communication or computational resources.

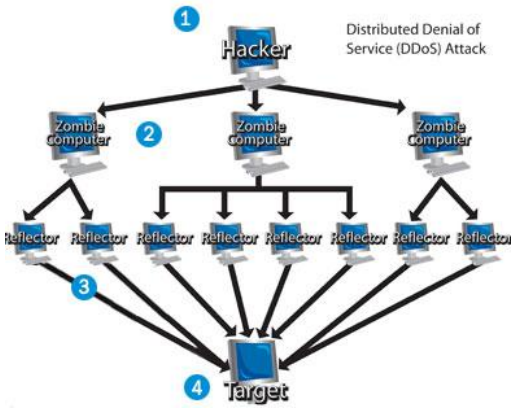

Fig. 1. An idea how an attack is carried out by a Hacker/Attacker

Attack Architectures: -

Two types of DDoS attack networks haveemerged: -

- **The Agent-Handler Model.**
- **The Internet Relay Chat (IRC) based Model.**

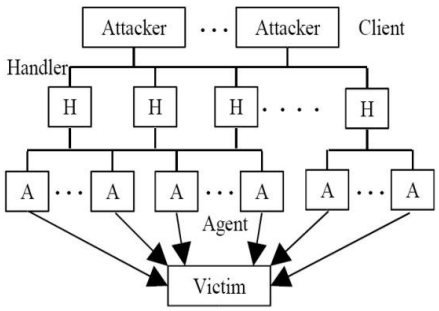

Fig. – 2:DDOS Agent-Handler Attack Model

International Journal of Innovative Research in Science and Engineering
Vol. No.2, Issue 04, April 2016
www.ijirse.com
ISSN: 2454-9665

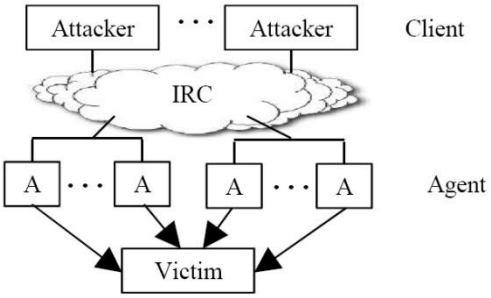

Fig. –3:DDOS IRC - based Attack Model

III. WHY DDOS ATTACKS

The question arises what is the need for conducting DDoS. The reason can possibly be anything, but some of the main reasons for which DDoS attacks are done arediscussed below. It is already clear that the attackers who plan the attacks and execute them are very qualified and have a great knowledge about computer and all its related issues right away ranging from architectural level to the application level. Thus, DDoS attacks are carried by Hackers who are exceptionally good at computers.

Generally, the attacker/hacker can be anyone in the world but recent surveys and analysis of previous attacks made clear the nature and motive of attacks by them. Thus, it was found that these hackers can be grouped according to their motives. About 90% of attacks can thus be classified and 10% rest hackers are negligible.

Thus the main classification of attackers/hackers according to their motive for DDoS attacks is as follows: -

- **The "Fun" Hackers**
- **The Activists**
- **The Terrorists**
- **Grey Area Competitors**

IV. VARIOUS TYPES OF DDoS ATTACKS

There are a wide variety of DDoS attacks. Wepropose here a categorization of the main DDoS attack methods. There are two main classes of DDoS attacks:-

- **Bandwidth Depletion Attack**
- **Resource Depletion Attack**

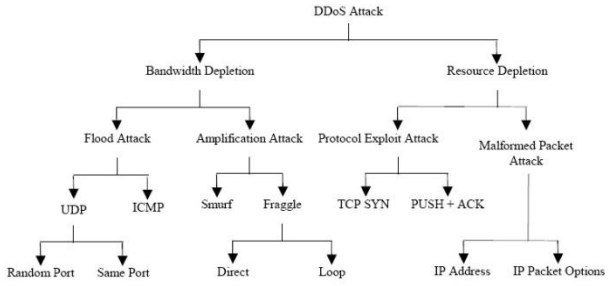

Fig. 3: - The detailed classification of types of DDoS Attacks

ISSN: 2454-9665

4.1 Bandwidth Depletion Attacks

Bandwidth depletion attacks can be characterizedas Flood Attacks and Amplification Attacks.

Flood Attacks: - A flood attackinvolves zombies sending large volumes of traffic to a victim system, to congest the victim

- system's network bandwidthwith IP traffic. The victim system slows down, crashes, orsuffers from saturated network bandwidth, preventingaccess by legitimate users. Flood attacks have beenlaunched using both UDP (User Datagram Protocol) andICMP (Internet Control Message Protocol) packets.

  In a **UDP Flood attack**, a large number of UDPpackets are sent to either random or specified ports on thevictim system. The victim system tries to process theincoming data to determine which applications haverequested data. If the victim system is not running any applications on the targeted port, it will send out an ICMPpacket to the sending system indicating a "destination portunreachable" message.

  Often, the attacking DDoS tool will also spoofthe source IP address of the attacking packets. This helpshide the identity of the secondary victims since returnpackets from the victim system are not sent back to thezombies, but to the spoofed addresses. UDP flood attacksmay also fill the bandwidth of connections located aroundthe victim system. This often impacts systems located nearthe victim.

  An **ICMP flood attack**occurs when the zombiessend large volumes of ICMP_ECHO_REPLY packets("ping") to the victim system. These packets signal the victim system to reply and the combination of traffic saturates the bandwidth of the victim's networkconnection. During this attack, the source IP address ofthe ICMP packet may also be spoofed.

- **Amplification Attacks: -**An amplification attackinvolves the attacker or the zombies sending messages to abroadcast IP address, using this to cause all systems in thesubnet reached by the broadcast address to send a reply tothe victim system. The broadcast IP address feature isfound on most routers; when a sending system specifies abroadcast IP address as the destination address, the routersreplicate the packet and send it to all the IP addresseswithin the broadcast address range. In this attack, thebroadcast IP address is used to amplify and reflect theattack traffic, and thus reduce the victim system'sbandwidth.

  The attacker can send the broadcast messagedirectly, or use the agents to send the broadcast messageto increase the volume of attacking traffic. If the attacker decides to send the broadcast message directly, this attackprovides the attacker with the ability to use the systemswithin the broadcast network as zombies without needing to infiltrate them or install any agent software.

A DDoS**Smurf attack**is an example of anamplification attack where the attacker sends packets to anetwork amplifier (a system supporting broadcastaddressing), with the return address spoofed to thevictim's IP address. The attacking packets are typicallyICMP ECHO REQUESTs, which are packets (similar to a "ping") that request the receiver to generate an ICMPECHO REPLY packet.Theamplifier sends the ICMPECHO REQUEST packets to all of the systems within thebroadcast address range, and each of these systems will return an ICMP ECHO REPLY to the target victim's IPaddress. This type of attack amplifies the original packettens or hundreds of times.

Another example is the DDoS**Fraggle attack**, whereattackersendspackets to a network amplifier, usingUDP ECHO packets. There is a variation of theFraggle attack where the UDP ECHO packets are sent tothe port thatsupports character generation (chargen, port19 in UNIX systems), with the return addressspoofed tothe victim's echo service (echo, port 7 in UNIX systems)creating an infinite loop. The UDP Fraggle packet willtarget the character generator in the systems reached bythe broadcast address. These systems each generate acharacter to send to the echo service in the victim system,which will send an echo packet back to the charactergenerator, and the process repeats. This attack cangenerate more bad traffic and cause more damage than aSmurf attack.

4.2 Resource Depletion Attacks

They involve the attacker sending packets that misuse network protocol communications or are malformed. Network resources are tied up so that none are left for legitimate users.

- **Protocol Exploit Attacks**
- **Malformed Packet Attacks**

V. VARIOUS DDoS ATTACK TOOLS

Internet Security Systems (ISS) has identified a number of distributed denial of servicetools readily available on the Internet. Some of these attack tools include: TFN, Trin00,TFN2K, and Stacheldraht. These attack tools differ in their capabilities and complexities,but all share the common goal of
attempting to overwhelm a victim with an abundantamount of difficult to detect or filter traffic. The evolution of these tools has introducedboth encryption and additional tiers to avoid their detection and increase their scalability.

- **Tribal Flood Network (TFN)**

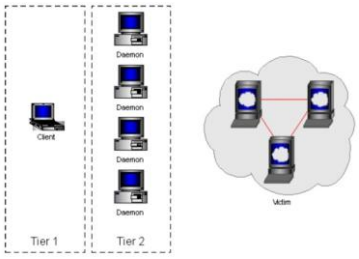

Fig. 4: Two-tier architecture of TFN

- **TRIN00**

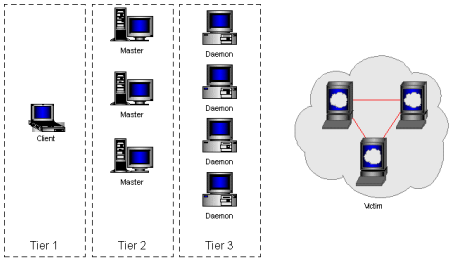

Fig. 5: Three-tier architecture of TRIN00

ISSN: 2454-9665

VI. ATTACK PROCEDURE OF DDoS

(Modus Operandi)

Operating systems and network protocols are developed without applying security engineering which in result provide hackers a lot of insecure machines on Internet.These insecure/unpatched machines are used by DDoSattackers as their army to launch attack as attacker gradually implants attack programs on these insecure machines. Depending upon sophistication in logic of implanted programs these compromised machines are called Handlers or Zombies and are collectively called bots and the attack network is called botnet in hacker's community. As shown in Fig. 2, the zombie machines under the control of handlers send attack packets which converge at victim or its n/w to exhaust either its communication or computational resources.

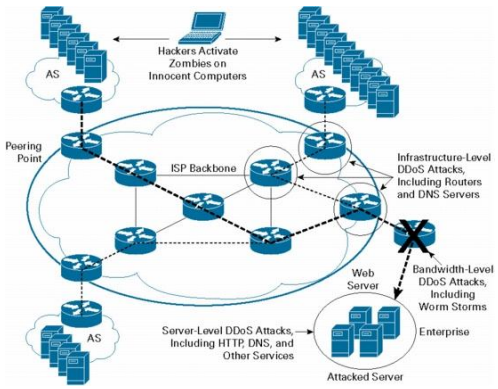

Fig. 6: Attack Procedure

VII. DEFENSE AGAINST DDoS ATTACKS

No defense mechanism or measure implemented is full-proof in any area, and this is no false in the case of DDoS attacks also. No matter how secure and efficient defense techniques are developed to secure the network,the attackers/hackers will manage to devise new and innovative methods to penetrate and implant the attacks.

Thus, as new and new attacks are discovered, their counter measures or defense techniques are designed accordingly.In short, no fail-safe solution is available to counter DDoS attacks.

- The attackers will manage to discover new methods of DDoS attacks by analyzing the weaknesses of protocols.
- The attackers exploit the defense mechanisms by generating false alarms and to cause catastrophic consequences.

In the area of Defense against DDoS, there are 2 approaches to it. They are: -

Preventive Measures

The goal of preventive defense mechanisms are:-

- To eliminate the possibility of DDoS attacks altogether, i.e., to design such defense techniques that

ISSN: 2454-9665

can judge the possible attacks and stop them from draining your system.

- To enablepotential victims to endure the attacks such that they don't stop providing services to legitimate users.

Thus there are mainly two types of prevention mechanisms: -

- **Attack Prevention Mechanisms: -**
  - **System Security**
  - **Protocol Security**

- **Denial-of-Service Prevention Mechanisms:**
  - **Resource Accounting**
  - **Resource Multiplication**

Reactive Measures

- Reactive measures strive to alleviate the impact of an attack on the victim. In order to attain this goal they need to detect the attack and respond to it.
- The goal of attack detection is to detect every attempted DDoS attack as early as possible.
- Upon attack detection, steps can be taken to characterize the packets belonging to the attack stream and provide this characterization to the response mechanism
- The goal of the attack response is to relieve the impact of the attack on the victim, while imposing minimal collateral damage to legitimate clients of the victim.
- There are essentially two phases :
  - **Attack Detection**
  - **Response Strategy**

Now we will discuss each phase in detail.

Attack Detection: Pattern Attack Detection

- Mechanisms that deploy pattern detection store the signatures of known attacks in a database.
- Each communication is monitored and compared with database entries to discover occurrences of DDoS attacks.
- Occasionally, the database is updated with new attack signatures.
- The obvious drawback of this detection mechanism is that it can only detect known attacks, and it is usually helpless against new attacks or even slight variations of old attacks that cannot be matched to the stored signature.
- On the other hand, known attacks are easily and reliably detected.

Response Strategy: Rate Filtering Mechanism

- Filtering mechanisms use the characterization provided by a detection mechanism to filter out the attack stream completely.

ISSN: 2454-9665

- Examples include dynamically deployed firewalls
- Unless detection strategy is very reliable, filtering mechanisms run the risk of accidentally denying service to legitimate traffic.
- Worse, clever attackers might leverage them as denial-of-service tools.

VIII. CONCLUSION

- Distributed denial of service attacks are a complex and serious problem, and consequently, numerous approaches have been proposed to counter them.
- DDoS attacks can be carried by anyone due to any reason but the major attackers include the "fun" hackers, terrorists, activists, etc. to spread chaos, terror or for their personal grudges.
- Majorly, there are 2 types of DDoS attacks which Bandwidth Depletion Attacks and Resource Depletion Attacks. Some of the various tools required to carry out DDoS are: - TFN, TRIN00, TFN2K and Stacheldraht.
- For defense against DDoS, two approaches are taken that are Preventive Measures and the Reactive Measures. The Preventive measures include applying security and methods that can judge possible DoS attack and stop it from being executed beforehand only whereas the Reactive measuresstrive to alleviate the impact of an attack on the victim. They detect the attack and then respond to it.
- Finally, A DDoS attack simulation was successfullydone by an internet security firm called HACKTICS for a big corporate client X. It showed that the whole internet sites of the client can be brought down by executing an appropriate attack script with the use of just 3 laptops.

REFERENCES

[1] CAMPBELL, T. A., AND IVANOVA, O. S. 2013. 3D printing of multifunctional nanocomposites. Nano Today 8, 2, 119 – 120.

[2] CHEN, D., LEVIN, D. I. W., DIDYK, P., SITTHI-AMORN, P., AND MATUSIK, W. 2013. Spec2Fab: A reducer-tuner model for translating specifications to 3D prints. ACM Trans. Graph. 32, 4, 135:1–135:10.

[3] CHO, W., SACHS, E. M., PATRIKALAKIS, N. M., AND TROXEL, D. E. 2003. A dithering algorithm for local composition control with three-dimensional printing. Computer-aided design 35, 9, 851–867.

[4] CHOI, J.-W., KIM, H.-C., AND WICKER, R. 2011. Multi-material stereolithography. Journal of Materials Processing Technology 211, 3, 318–328.

[5] DIMAS, L. S., BRATZEL, G. H., EYLON, I., AND BUEHLER, M. J. 2013. Tough composites inspired by mineralized natural materials: Computation, 3D printing, and testing. Advanced Functional Materials 23, 36, 4629–4638.

[6] Deif A (2012**)** Implementation of Lean tools and techniques in automotive industry. Journal of Applied Sciences 2012; 12(10):1032-37.

[7] Lewoc JB, Izworski A, Skowronski SF, Kieleczawa A and Kopacek, P. (2012) Emerging Smart Engineering: An Integrated Manufacturing and Management System. International Journal of Engineering Research and Applications 2012; 2(4):930-36.

[8] Masood T and Khan I.(2004) Productivity Improvement through Computer Integrated Manufacturing in Post WTO Scenario, National Conference on Emerging Technologies 2004.

[9] Moin CJ, Haque R and Mahabubuzzaman AK.(2010) A study on Computer integrated manufacturing method in Bangladeshi textile industry. Journal of Innovative development strategy. 2010; 4(1):5-11.

[10] Nagalingam SV and Lin GCI.(1999) Latest developments in CIM. Robotics and Computer Integrated Manufacturing 1999; 15:423-30.

[11] Titu MA, Oprean C and Grecu D. (2010) Applying the Kaizen Method and the 5S Technique in the Activity of Post-Sale Services in the Knowledge-Based Organization. Proceedings of the International Multi conference of engineers & computer scientists 2010; 3:978-88.

[12] Upadhye N, Deshmukh SG, Garg S. (2010) Lean manufacturing system for medium size manufacturing enterprises: an Indian case. International Journal of Management Science and Engineering Management 2010; 5(5):362-75.

[13] Veeramani D, Tserng HP, Russell JS.(1998) Computer-integrated collaborative design and operation in the construction industry. Automation in Construction 1998; 7:485-92.

[14] DONG, Y., WANG, J., PELLACINI, F., TONG, X., AND GUO, B. 2010. Fabricating spatially-varying subsurface scattering. ACM Trans. Graph. 29, 4, 62:1–62:10.

[15] DUBOIS, A., GRIEVE, K., MONERON, G., LECAQUE, R., VABRE, L., AND BOCCARA, C. 2004. Ultrahigh-resolution full-field optical coherence tomography. Appl. Opt. 43, 14 (May), 2874– 2883.

[16] HAN, L.-H., SURI, S., AND SCHMIDT, C. E. 2010. Fabrication of three-dimensional scaffolds for heterogeneous tissue engineering. Biomed Microdevices 12, 721–725.

[17] HAŠAN, M., FUCHS, M., MATUSIK, W., PFISTER, H., AND RUSINKIEWICZ, S. 2010. Physical reproduction of materials with specified subsurface scattering. ACM Trans. Graph. 29, 4, 61:1–61:10.

[18] HILLER, J. D., AND LIPSON, H. 2012. Automatic design and manufacture of soft robots. IEEE Transactions on Robotics 28, 2, 457–466.