ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Classification of Distributed Denial of Service Attacks – Architecture, Taxonomy and Tools

[I]Lovepreet Kaur Somal, [II]Karanpreet Singh Virk
[I,II]M.Tech Student, Dept. of Computer Engineering, Punjabi University Patiala, Punjab, India

Abstarct
Denial of Service (DoS) attack is a malicious effort to keep endorsed users of a website or web service from accessing it, or limiting their ability to do so. A Distributed Denial of Service (DDoS) attack is a type of DoS attack in which many computers are used to cripple a web page, website or web-based service. Fault either in users' implementation of a network or in the standard specification of protocols has resulted in gaps that allow various kinds of network attack to be launched of the type of network attacks, denial-of-service flood attacks have reason the most severe impact. In particular, we describe network based and host based DoS attack techniques to illustrate attack principles. DoS attacks are classified according to their major attack characteristics .In this paper the history and the recent trends of the DDoS attacks ,strategy of the DDoS attacks ,taxonomy of the attacks and the various tools which are used to implement the DDoS attacks have been discussed.

Keywords
DoS, DDoS, network, host, attack taxonomy, integrated approach

I. Introduction

Distributed denial-of-service attacks (DDoS) pose an immense threat to the Internet, and consequently many defense mechanisms have been proposed to combat them. Attackers constantly modify their tools to bypass these security systems, and researchers in turn modify their approaches to handle new attacks. The DDoS field is evolving quickly, and it is becoming increasingly hard to grasp a global view of the problem[1] This paper strives to introduce some structure to the DDoS field by developing a taxonomy of DDoS attacks and DDoS defense systems. The goal of the paper is to highlight the important features of both attack and security mechanisms and stimulate discussions that might lead to a better understanding of the DDoS problem[1] .A Denial of Service attack is an attempt by a person or a group of persons to cripple an online service. This can have serious consequences, especially for companies like Amazon and eBay which rely on their online availability to do business. In the not so distant past there have been some large scale attacks targeting high profile internet sites [2, 3, 4, and 5]. Consequently, there are currently a lot of efforts being made to come up with mechanisms to detect and mitigate such attacks. Even though the first denial of service attacks did not take place a long time ago (tools that automate setting up of an attack network and launching of attacks, started appearing in 1998), there are a multitude of denial of service attacks that have been used. Broadly speaking the attacks can be of three forms. a) Attacks exploiting some vulnerability or implementation bug in the software implementation of a service to bring that down. b) Attacks that use up all the available resources at the target machine. c) Attacks that consume all the bandwidth available to the victim machine. The third type of attacks is called bandwidth attacks[1]. A distributed framework becomes especially suited for such attacks as a reasonable amount of data directed from a number of hosts can generate a lot of traffic at and near the target machine, clogging all the routes to the victim. Protection against such large scale distributed bandwidth attacks is one of the most difficult (and urgent) problem to address in today's internet. CERT reports bandwidth attacks as increasingly being the most common form of Denial of Service attacks seen in the internet today[1]

II. History And Trends In Ddos Attacks

The DDoS attacks gained very widespread notoriety and media exposure with the three days of DoS attacks[6,7,8,9] (Feb 7-11, 2000) that were launched against major internet sites like CNN, Yahoo, EBay and Datek. Multiple attack tools like Trinoo, TFN, StachleDraht, TFN2K were used in these attacks. Ironically, these attacks came just a day after Steve Bellovin.s talk on Distributed Denial of Service at NANOG (North American Network Operator.s Group) in San Jose. But, Denial of Service attacks had been observed, studied and some attack tools like Trinoo and TFN even analyzed much before the infamous week. The sophistication of the DDoS attack tools has kept on improving with time. Therefore a historical study of DDoS attacks also gives a good overview of the various techniques that are used in orchestrating such attacks. This section starts off with an explanation of the various steps involved in orchestrating a DDoS attack. We then move on to look at the various attack tools available and study how these tools evolved over time [10].

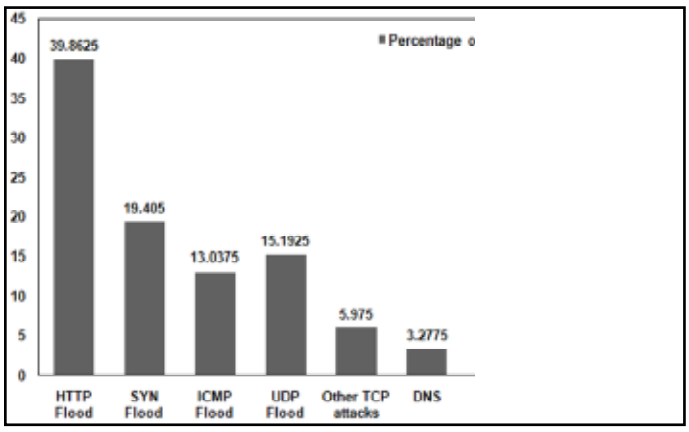

Fig. 1: DDoS attacks statistics by type[12] for 2011 [11]

III.DDOS Attack Architectures

As stated in [13], a DDoS attack can be defined as an attack which uses a large number of computers to launch a coordinated DoS attack against a single machine or multiple victim machines. Using client/server technology, the perpetrator is able to multiply the effectiveness of the DoS attack significantly by harnessing the

resources of multiple unwitting accomplice computers, which serve as attack platforms. Rather than breaking the victim's defense system for fun or to show prowess, a DDoS attack aims to cause damage on a victim either for personal reasons, material gain, or for popularity. We see in the taxonomy that intruders attempt to launch DDoS attacks based on exploitation of various means and their resultant effects can be observed at various levels or magnitudes. DDoS attacks mainly take advantage of the architecture of the Internet and this is what makes them powerful. While designing the Internet, the prime concern was to provide for functionality, not security. As a result, many security issues have been raised, which are exploited by attackers. Some of the issues are given below.

- Internet security is highly interdependent. No matter how secure a victim's system may be, whether or not this system will be a DDoS victim depends on the rest of the global Internet [14, 15].
- Internet resources are limited. Every Internet host has limited resources that sooner or later can be exhausted by a sufficiently large number of users.
- Many against a few: If the resources of the attackers are greater than the resources of the victims, the success of the attack is almost definite.

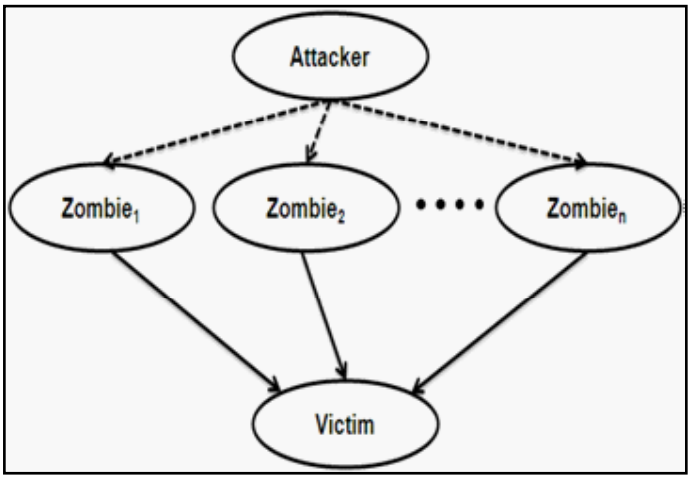

Fig 2: Direct DDoS attack: Send control traffic directly to the zombies to attack the victim host[12]

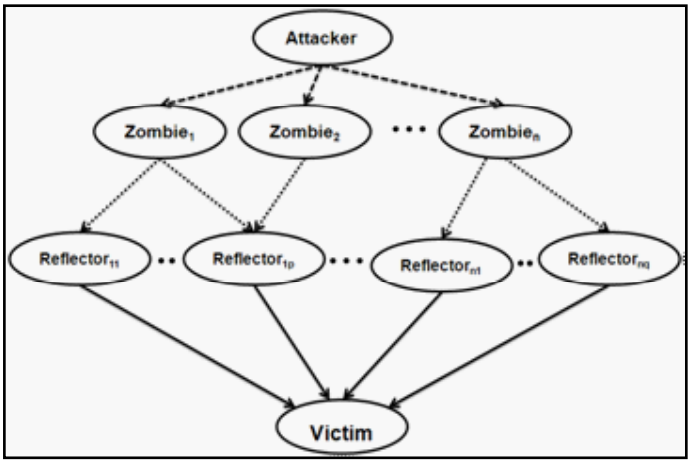

Fig3:Indirect DDoS attack: Send control traffic indirectly to the zombies to compromise the target host. Reflectors are non-compromised systems that exclusively send replies to a request. [12]

V. DDoS Strategy

A Distributed Denial of Service (DDoS) attack is composed of several elements. There are several steps in launching a DDoS attack.

1. Selection of agents

The attacker chooses the agents that will perform the attack. Based on the nature of vulnerabilities present, some machines are compromised to use as agents. Attackers victimize these machines, which have abundant resources, so that a powerful attack stream can be generated. In early years, the attackers attempted to acquire control of these machines manually. However, with the development of advanced security tool(s), it has become easier to identify these machines automatically and instantly [12]

2. Compromise

The attacker exploits security holes and vulnerabilities of the agent machines and plants the attack code. Not only that, the attacker also takes necessary steps to protect the planted code from identification and deactivation. As per the direct DDoS attack strategy, shown in Figure 3, the compromised nodes, i.e., zombies between the attacker and victim are recruited unwitting accomplice hosts from a large number of unprotected hosts connected through the Internet in high bandwidth. On the other hand, the DDoS attack strategy is more complex due to inclusion of intermediate layer(s) between the zombies and victim(s). It further complicates the trace back mostly due to (i) complexity in untangling the trace back information (partial) with reference to multiple sources, and/or (ii) having to connect a large number of routers or servers.

3. Communication

The attacker communicates with any number of handlers to identify which agents are up and running, when to schedule attacks, or when to upgrade agents. Such communications among the attackers and handlers can be via various protocols, such as ICMP, TCP, or UDP. Based on configuration of the attack network, agents can communicate with a single handler or multiple handlers [12]

4. Attack

The attacker initiates the attack. The victim, the duration of the attack as well as special features of the attack such as the type, length, TTL, and port numbers can be adjusted. If there are substantial variations in the properties of attack packets, it is beneficial to the attacker, since it complicates detection.[12]

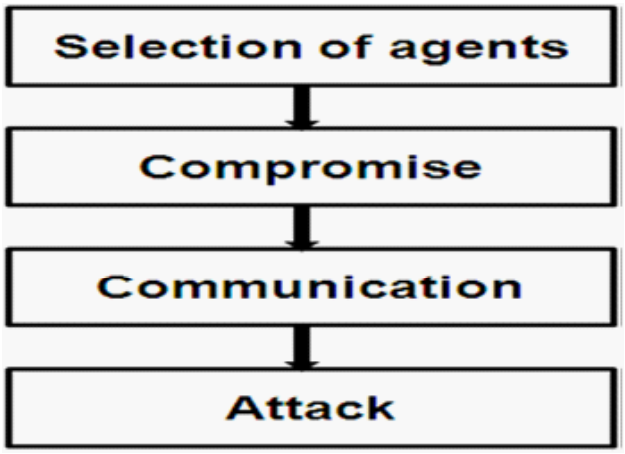

Fig. 4 : Steps to perform a DDoS attack[12]

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

VI. DDoS Attacks Taxonomy

There are a wide variety of DDoS attacks. We propose a taxonomy of the main DDoS attack methods There are two main classes of DDoS attacks: bandwidth depletion and resource depletion attacks. A bandwidth depletion attack is designed to flood the victim network with unwanted traffic that prevents legitimate traffic from reaching the primary victim. A resource depletion attack is an attack that is designed to tie up the resources of a victim system making the victim unable to process legitimate requests for service.[16]

Bandwidth Depletion Attacks

Bandwidth depletion attacks can be characterized as flood attacks and amplification attacks.

Flood Attacks

A flood attack involves zombies sending large volumes of traffic to a victim system, to congest the victim system's network bandwidth with IP traffic. The victim system slows down, crashes, or suffers from saturated network bandwidth, preventing access by legitimate users. Flood attacks have been launched using both UDP (User Datagram Protocol) and ICMP (Internet Control Message Protocol) packets. In a UDP Flood attack, a large number of UDP packets are sent to either random or specified ports on the victim system. The victim system tries to process the incoming data to determine which applications have requested data. If the victim system is not running any applications on the targeted port, it will send out an ICMP packet to the sending system indicating a "destination port unreachable" message [5]. Often, the attacking DDoS tool will also spoof the source IP address of the attacking packets. This helps hide the identity of the secondary victims since return packets from the victim system are not sent back to the zombies, but to the spoofed addresses. UDP flood attacks may also fill the bandwidth of connections located around the victim system. This often impacts systems located near the victim [16]

Amplification Attacks

An amplification attack involves the attacker or the zombies sending messages to a broadcast IP address, using this to cause all systems in the subnet reached by the broadcast address to send a reply to the victim system. The broadcast IP address feature is found on most routers; when a sending system specifies a broadcast IP address as the destination address, the routers replicate the packet and send it to all the IP addresses within the broadcast address range. In this attack, the broadcast IP address is used to amplify and reflect the attack traffic, and thus reduce the victim system's bandwidth. [16]

Resource Depletion Attacks

DDoS resource depletion attacks 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 .[16]

Protocol Exploit Attacks

We give two examples, one misusing the TCP SYN (Transfer Control Protocol Synchronize) protocol, and the other misusing the PUSH+ACK protocol. In a DDoS TCP SYN attack, the attacker instructs the zombies to send bogus TCP SYN requests to a victim server in order to tie up the server's processor resources, and hence prevent the server from responding to legitimate requests. The TCP SYN attack exploits the three-way handshake between the sending system and the receiving system by sending large volumes of TCP SYN packets to the victim system with spoofed source IP addresses, so the victim system responds to a non requesting system with the ACK+SYN. When a large volume of SYN requests are being processed by a server and none of the ACK+SYN responses are returned, the server eventually runs out of processor and memory resources, and is unable to respond to legitimate users.[16]

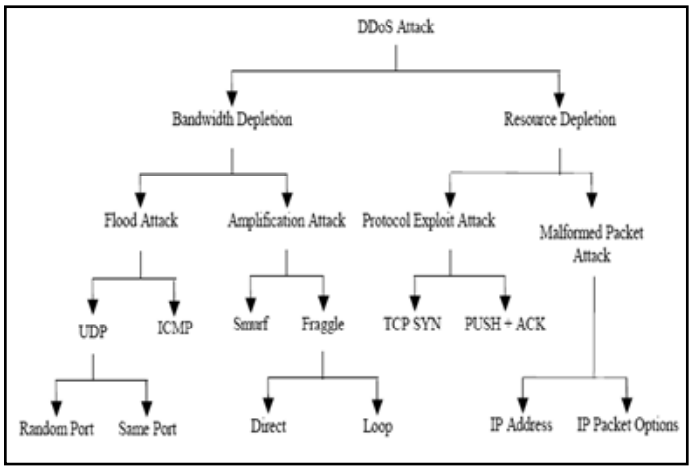

Fig. 5 : DDoS Attack Taxonomy [16]

Malformed Packet attacks

A malformed packet attack is an attack where the attacker instructs the zombies to send incorrectly formed IP packets to the victim system in order to crash it. There are at least two types of malformed packet attacks. In an IP address attack, the packet contains the same source and destination IP addresses. This can confuse the operating system of the victim system and can cause the victim system to crash. In an IP packet options attack, a malformed packet may randomize the optional fields within an IP packet and set all quality of service bits to one so that the victim system must use additional processing time to analyze the traffic. If this attack is multiplied, it can exhaust the processing ability of the victim system [16]

VII. DDOS Attack Tools

One of the major reason that make the DDoS attacks wide spread and easy in the Internet is the availability of attacking tools and the powerfulness of these tools to generate attacking traffic[17]. There are a variety of different DDoS attack tools on the Internet that allow attackers to execute attacks on the target system. Some of the most common tools are discussed below:

1)Trinoo [18, 19] can be used to launch a coordinated UDP flooding attack against target system. Trinoo deploys master/ slave architecture and attacker controls a number of Trinoo master machines. Communication between attacker and master and between master and slave is performed through TCP and UDP protocol, respectively.

2)TFN [20] uses a command line interface to communicate between the attacker and the control master program but offers no encryption between attacker and masters or between masters and slaves. Communication between the control masters and slaves is done via ICMP echo reply packets. It can implement Smurf, SYN Flood, UDP Flood, and ICMP Flood attacks.

3)TFN2K [21] is a more advanced version of the primitive TFN network. It uses TCP, UDP, ICMP or all three to communicate

between the control master program and the slave machines. TFN2K can implement Smurf, SYN, UDP, and ICMP Flood attacks. Communication between the real attacker and control master is encrypted using a key-based CAST-256 algorithm. In addition to flooding, TFN2K can also perform some vulnerability attacks by sending malformed or invalid packets.

4) Stacheldraht [22] combines best features of both Trinoo and TFN. It also has the ability to perform updates on the slave machines automatically. It uses an encrypted TCP connection for communication between the attacker and master control program. Communication between the master control program and attack daemons is conducted using TCP and ICMP. Stacheldraht can implement Smurf, SYN Flood, UDP Flood, and ICMP Flood attacks.

5) Shaft [23] has been modeled on Trinoo network. Other than the port numbers being used for communication International Journal of Computer and Electrical Engineering, Vol. 2, No. 2, April, 2010 1793-8163 271 purpose, working of it is very similar to the Trinoo. Thus, distinctive feature of Shaft is the ability to switch control master servers and ports in real time, hence making detection by intrusion detection tools difficult. Communication between the control masters and slave machines is achieved using UDP packets. The control masters and the attacker communicate via a simple TCP telnet connection. Shaft can implement UDP, ICMP, and TCP flooding attack.

6) Mstream [24] is more primitive than any of the other DDoS tools. It attacks target machine with a TCP ACK flood. Communication is not encrypted and is performed through TCP and UDP packets and the master connects via telnet to zombie. Masters can be controlled remotely by one or more attackers using a password protected interactive login. Source addresses in attack packets are spoofed at random. Unlike other DDoS tools, here, masters are informed of access, successful or not, by competing parties.

7) Knight [25] uses IRC as a control channel. It has been reported that the tool is commonly being installed on machines that were previously compromised by the BackOrifice Trojan horse program. Knight can implement SYN attacks, UDP Flood attacks, and an urgent pointer flooder [19]. It is designed to run on Windows operating systems and has features such as an automatic updater via http or ftp, a checksum generator and more.

8) Trinity [26, 27] is also IRC based DDoS attack tool. It can implement UDP, IP fragment, TCP SYN, TCP RST, TCP ACK, and other flooding attacks. Each trinity compromise machine joins a specified IRC channel and waits for commands. Use of legitimate IRC service for communication between attacker and agents eliminates the need for a master machine and elevates the level of the threat.

VI. Conclusion

In this paper the overview on the DDoS attacks has been represented. The various attacks and tools have been represented for the implementation of the DDoS attacks. Distributed denial of service attacks is a complex and serious problem and consequently, numerous approaches have been proposed to counter them. It is important to recognize and understand trends in attack technology in order to effectively and appropriately evolve defense and response strategies.

Thus, these taxonomies are likely to require expansion and refinement as new threats and defense mechanisms are discovered. The DDoS attack and DDoS attack tools outlined in this paper are useful to the extent that they clarify our thinking and guide us to more effective solutions to the problem of DDoS.

ACKNOWLEDGEMENT

The author is thankful to Karanpreet Singh Virk Department of Computer Engineering , Punjabi University , Patiala for his support .

Refrences

[1] DDoS Attacks Impact on Network Traffic and its Detection Approach 1Anup Bhange, 2Amber Syad, 3Satyendra Singh Thakur 1M.tech Scholar, Dept of CSE 2 Asst Prof, Dept of CSE 3Asst Prof, Dept of CSE 1,2 Patel Institute of Technology, Bhopal 3Patel college of Science Technology, Bhopal

[2] CNN. Cyber-attacks batter Web heavyweights, February2000/ www.cnn.com/2000/TECH/computing/02/0 /cyber.attacks

[3] CNN .Immense. Network assault takes down Yahoo, February http://www.cnn.com

[4] Netscape. Leading web sites under attack, February 2000 technews.netscape.com "Journal of Computer Science

[5] CERT coordination center. Denial of Service attacks http:// www.cert.org/tech_tips/denial_of_service.html

[6] CNN. Cyber-attacks batter Web heavyweight February2000. Available at http://www.cnn.com/2000/TECH/ computing/02/09/cyber.attacks.01/index.html.

[7] CNN .Immense. network assault takes down Yahoo, February2000.Available at http://www.cnn.com/2000/ TECH/computing/02/08/yahoo.assault.idg/index.html.

[8] Netscape. Leading web sites under attack, February 2000. Availableat http://technews.netscape.com/news/0-1007-200-1545348.html.

[9] CERT coordination center. Denial of Service attacks. http:// www.cert.org/tech_tips/denial_of_service.html

[10] A Survey of DDoS attacks and some DDoS defense Mechanism by Puneet Zaroo.

[11] Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions Monowar H. Bhuyan1, H. J. Kashyap1, D. K. Bhattacharyya1 and J. K. Kalita2 1Department of Computer Science & Engineering,Tezpur University, Napaam, Tezpur-784028, Assam, India 2Department of Computer Science, University of Colorado at Colorado Springs, CO 80933-7150, USA Email: {mhb,dkb}@tezu.ernet.in, jkalita@uccs.edu

[12] Kaspersky (2012). Kaspersky Internet Security & Anti-virus. http://www.kaspersky.com/. Russian Federation

[13] Stein, L. D. and Stewart, J. N. (2002). The world wide websecurity FAQ, version 3.1.2. http://www.w3.org/Security/ Faq. Cold Spring Harbor, NY.

[14] Houle, K. J. and Weaver, G. M. (2001) Trends in denial of service attack technology. Technical Report v1.0. CERT and CERT coordination center, Carnegie Mellon University, Pittsburgh, PA.

[15] Wong, T. Y., Law, K. T., Lui, J. C. S., and Wong, M. H. (2006) An efficient distributed algorithm to identify and traceback DDoS traffic. Comp. J., 49, 418–442.

[16] Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures Stephen M. Specht Electrical Engineering Princeton University

[17] Princeton, NJ 08544 stephen.specht@us.army.mil Ruby B. Lee Electrical Engineering Princeton University Princeton, NJ 08544 rblee@princeton.edu

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

[18] *Distributed Denial of Service Prevention Techniques B. B. Gupta, Student Member, IEEE, R. C. Joshi, and Manoj Misra, Member, IEEE .*

[19] *D. Dittrich, "The DoS Project's Trinoo Distributed Denial of Service attack tool," University of Washington, October 21, 1999. Available at: http://staff.washington.edu/dittrich/ misc/ trinoo.analysis.txt.*

[20] *D. Dittrich, "The Tribe Flood Network Distributed Denial of Service attack tool," University of Washington, October 21, 1999. Available at: http://staff.washington.edu/dittrich/ misc/tfn.analysis.*

[21] *J. Barlow, W. Thrower, "TFN2K- An Analysis," Axent Security Team. February 10, 2000. Available at: http:// security.royans.net/info/posts/bugtraq_ddos2.shtml.*

[22] *D. Dittrich, "The Stacheldraht Distributed Denial of Service attack tool," University of Washington, December 1999. Available at: http://staff.washington.edu/dittrich/misc/ stacheldraht.analysis.txt.*

[23] *S. Dietrich, N. Long, D. Dittrich, "Analyzing Distributed Denial of Service tools: The Shaft Case," in Proceedings of the 14th Systems Administration Conference (LISA 2000), New Orleans, LA, USA, pp. 329-339, December 3–8, 2000.*

[24] *D. Dittrich, G. Weaver, S. Dietrich, and N. Long, "The "Mstream" distributed denial of service attack too," May 2000. Available at: http://staff.washington.edu/dittrich/ misc/mstream.analysis.txt.*

[25] *Bysin, "Knight.c sourcecode," PacketStormSecurity.nl, July11,2001.Availableat:http://packetstormsecurity.nl/ distributed/ knight.c.*

[26] *B. Hancock, "Trinity v3, a DDoS tool," hits the streets, Computers Security 19(7), pp. 574, 2000.*

[27] *M. Marchesseau, ,,Trinity-Distributed Denial of Service Attack Tool," 11 Sept, 2000. Available at: http://www.giac. org/certified_professionals/practicals/gsec/0123.php*

Lovepreet Kaur is a M.Tech student at Department of Computer Engineering at Punjabi university Patiala. Her research interests include network security and DDoS attacks.

Karanpreet Singh Virk is a M.Tech student at Department of Computer Engineering, Punjabi University Patiala. His research interests include network security, RED algorithm and DDoS attacks.