A Study of DDOS Attacks, Tools and DDOS Defense Mechanisms

Nitin Gupta[1], Meenu Dhiman[2]

Department of Information Technology,
Maharishi Markandeshwar University, Mullana, Ambala, India

***Abstract*—This paper proposes a study of distributed denial-of service attacks and a study of the defense mechanism that strive to counter these attacks. The attack illustrate do using both known and potential attack mechanisms along with this classification we discuss important feature .So each attack category that in turn define the challenge involved in combating these threats. Distributed Denial of Service (DDOS) attacks**

Have become a large problem for users of computer Systems connected to the Internet. DDOS attackers hijack secondary victim systems using them to wage a

Coordinated large-scale attack against primary victim systems.

***Keywords*—DDOS , Defense , Denial of services.**

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. This paper strives to introduce some structure to the DDOS field by developing taxonomy of DDOS attacks and DDOS defense systems [3, 8].

DDOS attacks are relatively new and not well understood. This paper proposes taxonomy for understanding different DDOS attacks, tools and countermeasures [9]. We hope these taxonomy aids in perceptive the scope of DDOS attacks leading to more comprehensive solutions or countermeasures to cover both known attacks and those that have not yet occurred[1,3]. This paper is also the first to characterize the setup and installation techniques of DDOS attack architectures.

DDOS means there are more than one object which is DOS attacker (either automated tools or human) [12]. A DDOS attacker can greatly reduce the quality of a target internet service or even can completely break the network connectivity of a server generally to achieve resource overloading, a DDOS attacker will first compromise a large number of

hosts and subsequently instruct this compromised host to attack the service by exhausting a target resource [5, 7].

In Feb. 2000, a string of DDOS attacks crippled popular with sites including CNN.com, yahoo.com, eBay.com for several hours [4, 11, 13]. In 2003, for example, one honey pot research project saw 15,164 unique zombies from a large botnet within days. In 2004, the witty worm created 12,000 zombies within 45min. IP spoofing has often been exploited by DDOS attack to 1) conceal flooding sources and dilute localities in flooding traffic 2) coax legitimate host into becoming reflectors redirecting and amplifying flooding traffic [5].

Analysts estimated that during the three hours Yahoo was down, it suffered a loss of e-commerce and advertising revenue that amounted to about $500,000. According to book seller Amazon.com, its widely publicized attack resulted in a loss of $600,000 during the 10 hours it was down. During their DDOS attacks, Buy.com went from 100% availability to 9.4%, while CNN.com's users went down to below 5% of normal volume and Zdnet.com and E*Trade.com were virtually unreachable. Schwab.com, the online venue of the discount broker Charles Schwab, was also hit but refused to give out exact figures for losses. One can only assume that to a company that does $2 billion dollars weekly in online trades, the downtime loss was huge. In a DDOS attack, the attacking packets come from tens or hundreds of addresses rather than just one, as in a "standard" DOS attack. Any DOS defense that is based upon monitoring the volume of packets coming from a single address or single network will then fail since the attacks come from all over. Rather than receiving, for example, a thousand gigantic Pings per second from an attacking site, the victim might receive one Ping per second from 1000 attacking sites.

II. Handle attacks

There are many approaches to handle DOS and DDOS attacks. These approaches address diverse aspects of these complex threats, such as attack prevention, detection or response. Still, there is not a common, comprehensive methodology to evaluate an impact of a DOS attack on a given network, or the performance of a given defense. Such a methodology is needed for the following reasons: To be able to protect systems from DDOS attack, we need ways to characterize how dangerous the attack is, to estimate the potential damage/cost from the attack to a specific network (with or without defense). Given many DDOS defenses, we need a common evaluation setting to evaluate and compare the performance of these defenses. These tests will also indicate a defense weak features that need improvement. This paper develops a common methodology for DDOS defense evaluation with the help of client approach.

DDOS benchmarks that represent a set of scenarios to be used for defense evaluation. A set of performance metrics that characterize an attack's impact and a defense's performance. A detailed specification of evaluation methodology, which provides guidelines on using and interpreting benchmarking results. The performance metrics that I have utilized are continuous measurement of TCP/IP communication through the use of commonly available tools in an operating system like ping, trace route, netdiag, path ping, IPSec, arp, DDOS software etc.

III. Benchmarking DDOS

There are some significant difficulties in creating a benchmark suite that will be able to capture all relevant DDOS attacks and later recreate them in a test bed. Since attackers continuously adjust their tools, relying on a set of attack features linked to a specific tool fails to detect novel attacks. Instead, we have to study attack dynamics and extract some fundamental features about the different types of DDOS attacks that are invariant of attack tools in the use. The first contribution of this paper is building of a set of automated tools that enable highly accurate attack detection and selection from a traffic trace. There is very little information about prevalent attacks in today's Internet.

This is mostly because there is no distributed monitoring infrastructure that could observe attacks in different parts of the Internet and correlate this information. Researchers have attempted to reduce Internet attack patterns from responses to spoofed traffic that reach a set of monitors that capture traffic sent to a dark address space (allocated to an organization but not used by a live host). This provides a valuable insight into attack patterns, but only for attacks that use spoofing. The second contribution of this thesis is that it provides means to deduce prevalent attack information by collecting attack samples from a vast number of publicly available traffic traces. We provide a preliminary step in this direction by applying our attack selection tools to several public traffic traces, and grouping selected attacks into meaningful clusters.

IV. Purposed Work

This paper describes the work on creating a collection of typical attacks, needed for "typical category" of the attack traffic component of DDOS benchmarks. This is accomplished by building a set of automatic tools that harvest this information from the public traffic traces – the DDOS toolkit. DDOS toolkits here indicate various tools that I have utilized in my practical study of DDOS. This paper will mainly focus on the methods to be protected from false attacks. The tools detect attacks in the trace, separate legitimate traffic going to the target from the attack traffic, and create attack samples that describe important attack features such as strength, type of the attack, number of sources etc.

I have utilized the Client–Server Approach in the Local LAN environment in which I have send lot of traffic to the server side than I have used the Connection analysis of these tools like IPSec and TCP/IP which are in built in an operating system and also with the help of other network analysis method. This tool provides a way to detect this unwanted traffic coming on the server. Simply the proper use of these network tools will help in getting a good idea and approach on how to get control of unwanted traffic from entering in a network. We have used a lot of connection analysis tools here below in a practical way to understand that how we can collect network information, statistics for DDOS. The tools we have utilized are ping, tracert, trace route, path ping, firewall, IP Security, Network Monitoring tools etc. We have utilized these tools and their output so that we can present the output of these tools for DDOS. We provide a preliminary step in this direction by applying our attack selection tools to several public traffic traces, and grouping selected attacks.

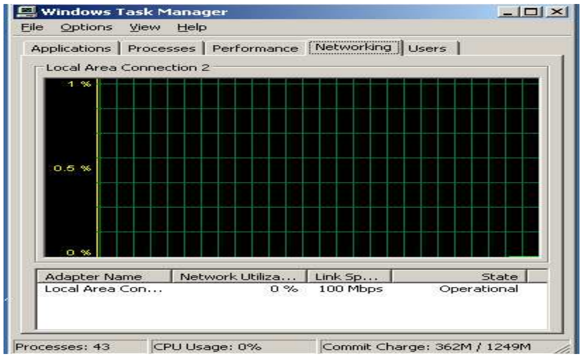
Attack selection process is performed in the following steps.

(1) Traffic filtering - It is defined as blocking unwanted traffic from entering into a network with a good network strategy.
(2) Attack Reaction - It is done using IPSec.
(3) Attack Detection - It provide a proper system monitoring, network performance with the help of monitoring tools to be graphical.

V. Results

IP Security is a main tool to defend against DDOS. IPSec can be used in the same way to defend a DNS server, HTTP Server, SMTP server and also we can make safe other services. In market there may be availability of various software which can be used for a better control of network attacks and can provide us more security. Ultimately in the end we have utilized the IP Security as the main tool to defend against DDOS. In this paper we mainly focus on the use of IPSec as the main tool for defense against DDOS.

We have used the windows task manager to understand the network performance from the following task Manager output.

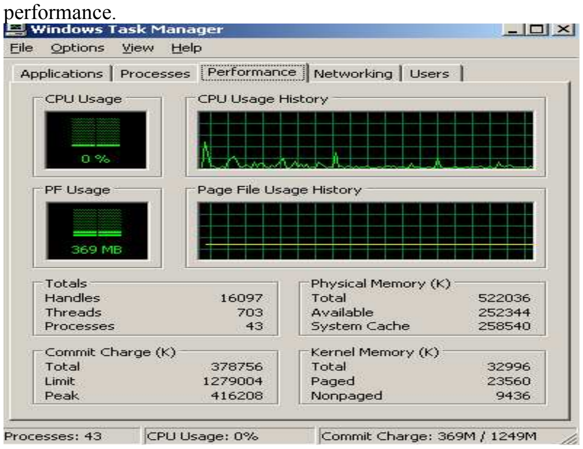


Adapter Name	Network Utiliza...	Link Sp...	State
Local Area Con...	0 %	100 Mbps	Operational

Processes: 43 CPU Usage: 0% Commit Charge: 362M / 1249M

Fig 1.1 Network Performances

The same task manager has been used to understand about the processing status of a server to get a better idea of the server performance.



Totals
Handles 16097
Threads 703
Processes 43

Physical Memory (K)
Total 522036
Available 252344
System Cache 258540

Commit Charge (K)
Total 378756
Limit 1279004
Peak 416208

Kernel Memory (K)
Total 32996
Paged 23560
Nonpaged 9436

Processes: 43 CPU Usage: 0% Commit Charge: 369M / 1249M

Fig 1.2 Server Performances

The same task manager can be used to get more about the processes running on the server and hence it can be a useful tool in order to decide about the planning defenses against unwanted attacks on a server. The tools are available in most server and client operating systems so we can use these tools for the planning of a better defense against the threats.

We have also performed the network monitoring. For network monitoring some connection parameters are used.

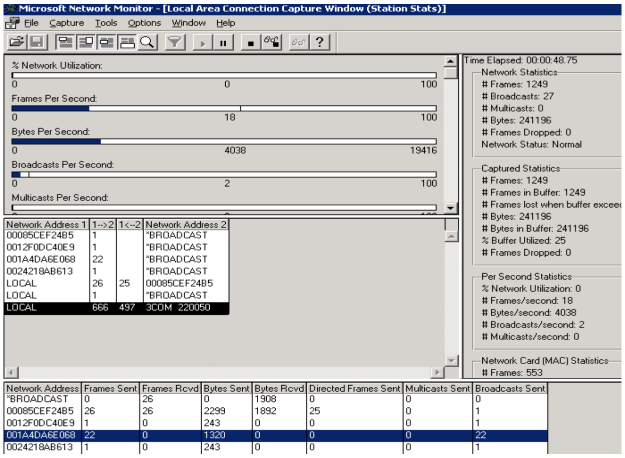
Each connection records the information Source IP, Destination IP, Source port, Destination port. A table called Destination table is used to keep information about every destination IP address observed in the trace and is accessed using the destination IP as a key. Sequence number of the first byte of the last packet , Sequence number of the last byte of the Last packet ,Legitimate flag, One –way flag ,Number of packets sent , Number of packets received ,Number of retransmissions , Number of fragmented packets, Suspicious points ,Timestamp of the last activity ,Number of bytes sent, Source IP, Destination IP, Source port, Destination port, Packet Destination Table Record.

In the support of the above matter we can use the following outputs taken in the local LAN. The following is the output of a normal ping command to mail.yahoo.com server on the internet. In this case of ping we are becoming the source and the yahoo server is the destination server. We can use a Network Monitor as more detailed network monitoring tool in support of our better analysis on DDOS, the output of ping can be used in testing connectivity as well as in making a server busy, the output of this command is shown below

```
C:\>ping mail.yahoo.com

Pinging in-inlogin.lgg1.b.yahoo.com [202.86.7.110] with 32 bytes
of data:
Reply from 202.86.7.110: bytes=32 time=58ms TTL=54
Reply from 202.86.7.110: bytes=32 time=58ms TTL=54
Reply from 202.86.7.110: bytes=32 time=58ms TTL=54
Reply from 202.86.7.110: bytes=32 time=57ms TTL=54
Ping statistics for 202.86.7.110:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 57ms, Maximum = 58ms, Average =
57ms
```

Output of a Network Monitor in support of this ping is given below:


Microsoft Network Monitor - [Local Area Connection Capture Window (Station Stats)]
File Capture Tools Options Window Help
?

% Network Utilization: 0 0 100
Frames Per Second: 0 18 100
Bytes Per Second: 0 4038 19416
Broadcasts Per Second: 0 2 100
Multicasts Per Second:

Time Elapsed: 00:00:48.75

Network Statistics
Frames: 1249
Broadcasts: 27
Multicasts: 0
Bytes: 241196
Frames Dropped: 0
Network Status: Normal

Captured Statistics
Frames: 1249
Frames in Buffer: 1249
Frames lost when buffer exceed
Bytes: 241196
Bytes in Buffer: 241196
% Buffer Utilized: 25
Frames Dropped: 0

Per Second Statistics
% Network Utilization: 0
Frames/second: 18
Bytes/second: 4038
Broadcasts/second: 2
Multicasts/second: 0

Network Card (MAC) Statistics
Frames: 553

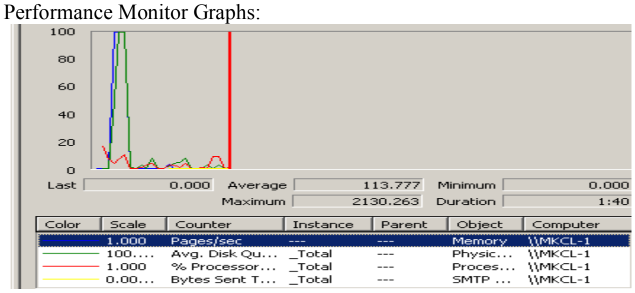
Network Address 1	1-->2	1<--2	Network Address 2
00085CEF24B5	1		*BROADCAST
0012F0DC40E9	1		*BROADCAST
001A4DA6E068	22		*BROADCAST
0024218AB613	1		*BROADCAST
LOCAL	26	25	00085CEF24B5
LOCAL	1		*BROADCAST
LOCAL	666	497	3COM 220050

Network Address	Frames Sent	Frames Rcvd	Bytes Sent	Bytes Rcvd	Directed Frames Sent	Multicasts Sent	Broadcasts Sent
*BROADCAST	0	26	0	1908	0	0	0
00085CEF24B5	26	26	2299	1892	25	0	1
0012F0DC40E9	1	0	243	0	0	0	1
001A4DA6E068	22	0	1320	0	0	0	22
0024218AB613	1	0	243	0	0	0	1

Fig 1.3 Network Monitor

Network Diagnostics also can be a better way to analyze network traffic coming on a server in support of Typical Network Monitor.

Analyzing performance of SMTP server with the help of Performance Monitor Graphs:



Last 0.000 Average 113.777 Minimum 0.000
Maximum 2130.263 Duration 1:40

Color	Scale	Counter	Instance	Parent	Object	Computer
🟦	1.000	Pages/sec	---	---	Memory	\\MKCL-1
🟩	100....	Avg. Disk Qu...	_Total	---	Physic...	\\MKCL-1
🟥	1.000	% Processor...	_Total	---	Proces...	\\MKCL-1
🟨	0.00...	Bytes Sent T...	_Total	---	SMTP ...	\\MKCL-1

Fig.1.4 Performance monitor graph

The above performance monitor graph shows that a yellow curve is used for the SMTP server; the level of utilization can be monitored at regular intervals for a better defense of the server.

I. Conclusion

In the end of my work upon the DDOS practices shown above that I have focused upon the available network tools in an operating system and freely available tools on internet, or the evaluation versions of the software's for the anti DDOS practices. DDOS practices can be given a more dedicated approach if we can utilize the Licensed versions of various software tools available for this purpose and by doing a continuous research on it by adopting an online approach. During the above work on DDOS my focus was to utilize only the available Network type tools for the fulfillment of DDOS.

II. References

[1] Mirkovic Jelena, Martin Janice and Reiher Peter (2004) , "A Taxonomy of DDOS attacks and DDOS defense Mechanisms". Computer Science Department. University of California, Los Angeles, Technical Report #020018.

.[2]Gao Zhiqiang, Ansari Nirwan, and Anantharam Karunakar, "A New Marking Scheme to Defend against Distributed Denial of Service Attacks", Department of Electrical and Computer Engineering, New Jersey Institute of Technology, Newark, NJ 07102, USA,2004.

[3] Specht Stephen M, Lee Ruby B(2004) , "Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures", Electrical Engineering, Princeton University Princeton, NJ 08544.

[4] Sachdeva1 Monika, Singh2 Gurvinder, Kumar1Krishan and Singh31 Kuldip (2008), "DDOS Incidents and their Impact: A Review" **,**Department of Computer Science and Engineering, SBS College of Engineering and Technology, India 2Department of Computer Science and Engineering, Guru Nanak Dev University, India 3Department of Electronics and Computer Engineering, Indian Institute of Technology, India

[5] Praveena V, and Kiruthika N (2008), "New Mitigating Technique to Overcome DDOS Attack"

[6] J. Postel, editor, "*Internet Protocol"*, RFC791 (1981).

[7] XIANG YANG and ZHOUWANLEI(2004),"Protecting Web Applications from DDOS Attacks by an Active Distributed Defense System *School of Engineering and Information Technology", Deakin University,221 Burwood Hwy, Burwood, 3125 Victoria, Australia*

[8]Vaughn Randal and Evron Gadi, " DNS Amplification Attacks", March 17, 2006

[9] Tucker C.J, " A new taxonomy for comparing intrusion detection systems" Internet Research Vol. 17 No. 1, 2007 ,pp. 88-98

[10] Onofrei Andreea Ancuta, Rebahi Yacine, Magedanz Thomas , "Preventing Distributed Denial-of-Service Attacks on the IMS Emergency Services Support through Adaptive Firewall Pinholing",The international journal of next generation network

[11] Vries Stephen de, "Surviving Distributed Denial of Service (DDOS) Attacks" , 11 February 2004

[12] Ballani Hitesh and Paul Francis(*CCS'08*, October 27{31, 2008), "Mitigating DNS DOS Attacks" ,Cornell University Ithaca, NY Cornell
. University Ithaca, NY

[13] Pu Calton(2007), "Denial of Information Attacks in Event Processing", School of Computer Science, Georgia Institute of Technology