Intrusion detection for ICMP- Flood attack

Anup Ingle [1] & Mohnish Awade.[2]

Abstract: **Increasing adoption of Internet technology worldwide has also increased stress on its privacy and security issue. There are many flaws such as Dos & DDoS attacks, DDOS- short for Distributed Denial of Service, cyber crimes, hacking, phishing came into existence. The losses, both, economical & social, were increased. The paper discuss the ICMP flood attackt connection and methods for prevention of penetration on internet. Using statistical Anomaly and Signature based Intrusion detection system for ICMP DDoS attack can be implemented on the software code may be on real time for ICMP- flood attack on target computers mainly computer using windows based operating system. The statistical implementation can be done using WEKA tool and attack generated by hping3.**

Keywords: **ICMP-Flood, DDoS, WEKA, Hping3, Statistical anomaly detection, Signature based anomaly detection.**

.

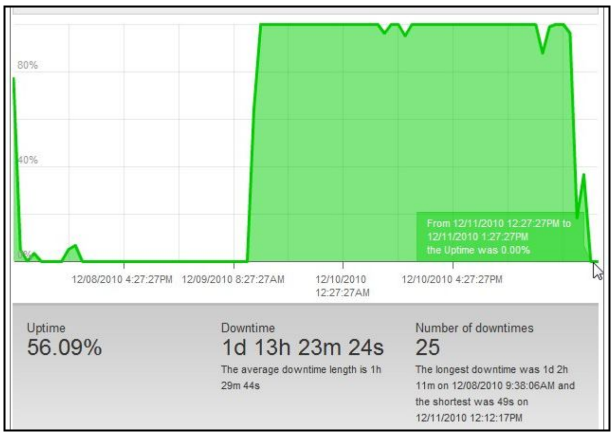
1. INTRODUCTION

With the evolution of internet there are many flaws like Dos & DDoS attacks, cyber crimes, hacking, phishing came into existence. The losses, both, economical & social, were increased. To summarize the severity of this attack here is the latest news from BBC news site "A Northampton student has been accused of taking part in a cyber attack that cost online payment portal PayPal £3.5 million. It is the prosecution case that Christopher Weatherhead is a cyber-attacker and that he, and others like him, waged a sophisticated and orchestrated campaign of online attacks that paralyzed a series of targeted computer systems." In this paper we will try to find the solution to the DDoS attack to be more particular the ICMP flood attack. We will use appropriate tool to generate such attach and try to identify possible solution for this type of attack.

2. DDoS ATTACK

DDOS, short for Distributed Denial of Service, is a type of DOS attack where multiple compromised systems -- which are usually infected with a Trojan -- are used to target a single system causing a Denial of Service (DoS) attack. Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack. According to this report on eSecurityPlanet, in a DDoS attack, the incoming traffic flooding the victim originates from many different sources – potentially hundreds of thousands or more. This effectively makes it impossible to stop the attack simply by blocking a single IP address; plus, it is very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin.

Out of all the categories of threat Dos & DDoS attacks were the most trivial & easy to conduct attacks, on the other hand the losses occurring because of them were severe. One of the severe losses caused because of these attacks is it brought down Visa, MasterCard and many other websites.



Uptime
56.09%

Downtime
1d 13h 23m 24s
The average downtime length is 1h 29m 44s

Number of downtimes
25
The longest downtime was 1d 2h 11m on 12/08/2010 9:38:06AM and the shortest was 49s on 12/11/2010 12:12:17PM

Figure1.1 A pictorial view of the damage created because of MasterCard Outrage

A report from Times of India published "Over 14,000 websites have been hacked by cyber criminals till October this year, an increase of nearly 57 per cent from 2010. To check hacking and cyber crimes, the government has conducted six cyber security mock drills since November 2009 to assess preparedness of organisations to withstand cyber attacks, minister of communications and IT Kapil Sibal had said in Parliament.

1. *Vishwakarma Institute of Information Technology, Pune.*

2. *Vishwakarma Institute of Information Technology, Pune.*

3. ICMP- FLOOD ATTACK

Most attractive and easy to operate ICMP based DDoS attacks are amplification attacks. Permitting ICMP traffic in a conservative manner will help defending the flooding attacks. Existing methods try to control the ICMP traffic with bandwidth limitation, sometimes the limitation is prodigal and in other cases the limitation is stringent which denies ICMP traffic completely even the vital usage. However the usage of ICMP over the Internet is necessary, therefore in this paper we identify the harmless rate at which the ICMP traffic can be generated resounded over the Internet. This harmless rate is achieved through ICMP window restriction scheme. We analyze and prove that the window restriction will remove the attack productivity region from the ICMP traffic and promotes only genuine traffic, thus helps to neutralize the flooding attacks. ICMP window restriction scheme therefore overcomes the issues concerning the unfair vertical limitation in bandwidth.

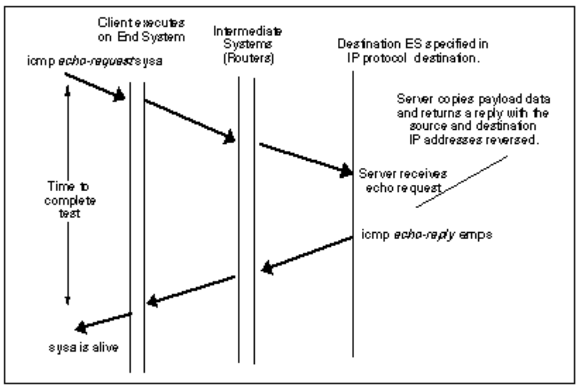

Client executes on End System
Intermediate Systems (Routers)
Destination ES specified in IP protocol destination.
icmp echo-request sysa
Server copies payload data and returns a reply with the source and destination IP addresses reversed.
Server receives echo request
Time to complete test
icmp echo-reply emps
sysa is alive

Figure3.1 shows the sequence of packets exchanged at the beginning of a normal ICMP connection

The ICMP flood attack sends ICMP connections requests faster than a machine can process them. Successful attacks left the system wide open for root access from anywhere on the Internet. A side effect of the attack is that a trusted system would ignore any packets received on the port that services remote log-in requests. The ICMP Flooding attack consists of a tool that only implements one portion of the Sequence Number Guessing attack, with a completely different focus. ICMP Flooding causes servers to quit responding to requests to open new connections with clients -- a denial of service attack.Out of various DDoS attack this is the chart of different type of DDoS attack.

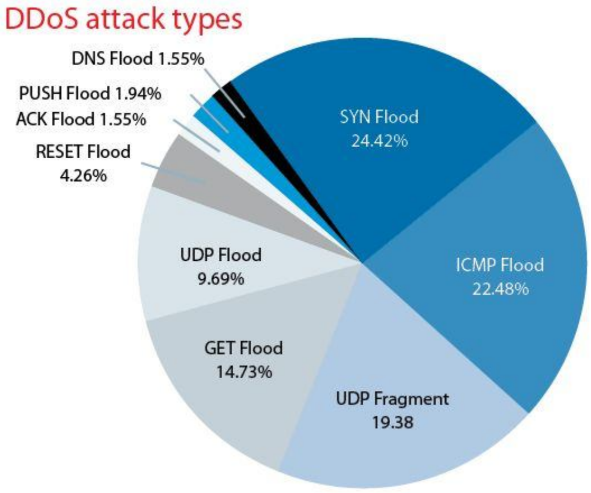


Figure 3.2 As per IT news survey in 2011 different type of DDoS attack

4. COMPLICATIONS IN ICMP-FLOOD ATTACK

There are various ways in which ICMP attack can be complicated; one of the techniques is shown below

A smurf attack is one particular variant of a flooding DoS attack on the public Internet. It relies on misconfigured network devices that allow packets to be sent to all computer hosts on a particular network via the broadcast address of the network, rather than a specific machine. The network then serves as a smurf amplifier. In such an attack, the perpetrators will send large numbers of IP packets with the source address faked to appear to be the address of the victim. The network's bandwidth is quickly used up, preventing legitimate packets from getting through to their destination.

Ping flood is based on sending the victim an overwhelming number of ping packets, usually using the "ping" command from Unix-like hosts (the -t flag on Windows systems has a far less malignant function). It is very simple to launch, the primary requirement being access to greater bandwidth than the victim.

Ping of death is based on sending the victim a malformed ping packet, which might lead to a system crash

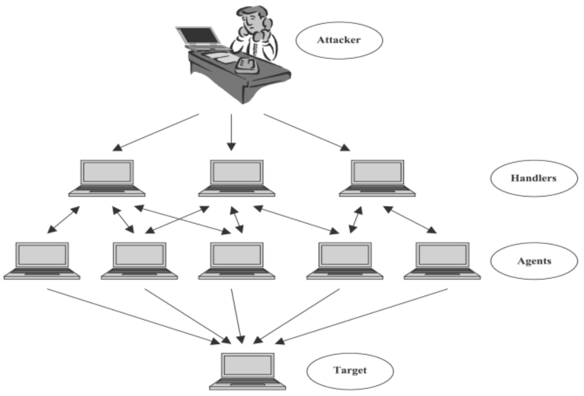


Figure 4.1 Attack demonstration of ICMP- flood

DDoS flooding attacks are quite popular with hackers and they can cause devastating impact on computer systems. Smurf attack is a type of flooding attack that involves ICMP protocol, which is known to have brought down high profile commercial websites. A computer system running Microsoft's Windows-XP with Service Pack2 (SP2) security software is designed to drop ICMP packets by default, which makes one believe that ICMP-based flooding attacks cannot harm a computer system that deploys SP2 security software. In this experimental paper, we set out to test and measure the effectiveness of the Microsoft Windows- XP with SP2 security software in protecting a computer system from ICMP-based flooding attacks in fast Ethernet environment. We simulate Smurf attacks on a computer system in the controlled lab environment. In these experiments, we measure the exhaustion of computing resource of a computer system with and without Windows-XP SP2 security software. It is observed that under Smurf attack, the victim computer deploying SP2 security software dropped all ICMP messages; nevertheless, the exhaustion of the processor resource of the computer running the SP2 security-software couldn't be stopped. Furthermore, it was found interestingly that the exhaustion of the processor resource of the computer system running the SP2 security was much higher than that of the computer system that didn't deploy SP2 security software. These experiments show that dropping of ICMP messages by SP2-security software at the victim computer is too late of an act in preventing the adverse effect of the Smurf attack. Once the attack traffic reaches the victim computer, SP2 security software is ineffective in preventing the resource exhaustion caused by the attack, even if it is configured to drop the ICMP messages.

I. Consequence of ICMP flood

Attacker creates a random source address for each packet. SYN flag set in each packet is a request to open a new connection to the server from the spoofed IP address. The victim responds to spoofed IP address, then waits for confirmation that never arrives (waits about 3 minutes) and victim's connection table fills up waiting for replies, soon after table fills up, all new connections are ignored legitimate users are ignored as well, and cannot access the server once attacker stops flooding server, it usually goes back to normal state as newer operating systems manage resources better, making it more difficult to overflow tables, but still are vulnerable SYN flood can be used as part of other attacks, such as disabling one side of a connection in ICMP hijacking, or by preventing authentication or logging between servers.

A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. There are two general forms of DoS attacks: those that crash services and those that flood services. A DoS attack can be perpetrated in a number of ways. The five basic types of attack are:

A. Consumption of computational resources, such as bandwidth, disk space, or processor time.

B. Disruption of configuration information, such as routing information.

C. Disruption of state information, such as unsolicited resetting of TCP sessions.

D. Disruption of physical network components.

E. Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

II. Statistical Anomaly and Signature based Intrusion detection system

All Intrusion Detection Systems use one of the two detection approach, i.e. Statistical Anomaly and Signature Based IDS

Statistical Anomaly-based IDS

A statistical anomaly-based ID establishes a performance baseline based on normal network traffic evaluations. It will then sample current network traffic activity to this baseline in order to detect whether or not it is within baseline parameters. If the sampled traffic is outside baseline parameters, an alarm will be triggered.

- Misuse Detection, use patterns of well-known attacks to identify intrusions:
- Record the specific patterns of intrusions
  Monitor current audit trails (event sequences) and pattern matching
- Report the matched events as intrusions

- Representation models: expert rules, Colored Petri Net, and state transition diagrams, etc.

a. Signature or Misuse-based IDS

Network traffic is examined for preconfigured and predetermined attack patterns known as signatures. Many attacks today have distinct signatures. In good security practice, a collection of these signatures must be constantly updated to mitigate emerging threats.

Anomaly detection, use deviation from normal usage patterns to identify intrusions:

- Establishing the normal behavior profiles
- Observing and comparing current activities with the (normal) profiles
- Reporting significant deviations as intrusions
- Statistical measures as behavior profiles: ordinal and categorical (binary and linear)

5. CONCLUSION

Using statistical Statistical Anomaly and Signature based Intrusion detection system for ICMP DDoS attack can be implemented on the software code may be on real time. Instead of having a huge database or requirement of high computation power for statistical pattern classification on real time network, the approach of classifying the intrusion traffic and then implementing it in the network as conclusion makes network intrusion monitoring faster and on real time. Statistical Anomaly and Signature based Intrusion detection system surely a promising solution for ICMP flood attack on target computers mainly computer using windows based operating system.

6. REFERENCES

[1] Erinc Arikan, "Attack Profiling for DDOS Benchmarks" A thesis submitted to the Computer and Information Sciences Faculty of the University of Delaware in partial fulfillment of the requirements for the degree of Master of Science with a major in Computer Science: Summer 2006.

[2] J. Udhayan and R. Anitha, "Demystifying and Rate Limiting ICMP hosted DOS/DDoS Flooding Attacks with Attack Productivity Analysis", 2009 IEEE International Advance Computing Conference (IACC 2009) Patiala, India, 6-7 March 2009.

[3] Matthew V. Mahoney and Philip K. Chan, "PHAD: Packet Header Anomaly Detection for Identifying Hostile Network Traffic", Florida Institute of Technology Technical Report CS-2001-04.

[4] Jie Wang, Raphael C.-W. Phan, John N. Whitley and David J. Parish, "DDoS Attacks Traffic and Flash Crowds Traffic Simulation with a Hardware Test Center Platform", 2011 IEEE.

[5] S. Kumar, M. Azad, O. Gomez, R. Valdez, "Can Microsoft's Service Pack2 (SP2) Security Software Prevent SMURF Attacks?", Proceedings of the Advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services,2006 IEEE.

[6] Jun Li, "Early Statistical Anomaly Intrusion Detection of DOS Attacks Using MIB Traffic Parameters", Proceedings of the 2003 IEEE Workshop on Information Assurance.

[7] Saad, Radwane; Nait-Abdesselam, Farid; Serhrouchni, Ahmed, "A collaborative peer-to-peer architecture to defend against DDoS attacks Local Computer Networks", 2008. LCN 2008. 33rd IEEE Conference on 14-17 Oct. 2008 Page(s):427 – 434.