Detection of DDoS attacks in Windows Communication Foundation services

S.Shalini, Rucha Wankhade, Priyanka Puriji, Reshmi Das,Vijendrasinh P.Thakur

Dept of Information Technology
YCCE,Nagpur
E-mail: sshalini1250@gmail.com

Abstract-- Internet provides many critical services so it has become very important to monitor the network traffic so that the resources of the network can be prevented from being depleted from malicious hackers. In this paper, we have presented a mechanism to detect and defense a web-server against a Distributed Denial of Service (DDoS) attack. We have presented simulation of specific kind of DDoS attack i.e. identity spoofing and SYN flood attack on an application similar to shopping portal and its results to demonstrate the effectiveness of the mechanism. Then, the attack is monitored in resource monitor of the server side monitor showing CPU utilization.Also,some defense mechanisms to defend the server against such attacks has been presented.

Keywords: *Network security, DDoS, IP spoofing, SYN flood attack.*

----------***----------

1. INTRODUCTION

Internet has become very famous nowadays which satisfies people with its various services which are related to various different fields. It provides a very versatile facility as with just few clicks one can complete many tasks easily and conveniently. Though it is the greatest tool for communicating in mass, but there is also a negative side of taking the help of Internet. Along with the popularity and rapid development of the Internet, network security issues become more and more serious [1]. Network security threats we face include: eaves dropping, denial-of-service attack, spoofing, illegally authorized access, and the spread of the virus etc. [1]

A denial of service (DoS) attack is a malicious attempt, which temporarily interrupts or suspends the services of a host connected to the Internet and makes the server or a network resource unavailable to users. In Distributed Denial of Service Attack (DDoS) the attack is "distributed" because the attacker is using multiple computers, including yours, to launch the denial-of-service attack.

Service-oriented applications can be build by using a framework known as Windows Communication Foundation (WCF) .Data as asynchronous messages can be send from one endpoint of service to another while using WCF. A service endpoint may be a part of a service which is continuously available and it is hosted by IIS, or it may be a service hosted in an application. An endpoint can be a client of a service that requests for some data from a service endpoint.

Spoofing is a type of scam where an intruder hiding its own identity pretends to be another user and tries to gain unauthorized access to that user's system or information. The main reason behind spoofing is to gain access to one's computer system, bank account or to steal personal information, such as passwords by tricking the user to reveal sensitive information.

This paper is organized as follows. Section 2, discusses the related work done on spoofing and DDoS attacks so far. Section 3, describes DDoS attacks and its effects and thorough explanation of TCP SYN flood attack in which our paper is based. The methodology of how the attack has been done on shopping portal application with results has been shown in section 4.Also some defense mechanisms to defend server against such attacks has been proposed in section 5.Finally, the paper has been concluded in Section 6.

2. RELATED WORK

In [2] paper has described various DDOS attacks which are broadly classified in two categories, one is protocol attacks and second volume based attacks. Resource depletion is occurred in protocol attacks which include attacks like TCP-SYN, ping of death, PUSH & ACK etc. Under volume based attacks there is depletion of bandwidth which includes flooding attacks like UDP, ICMP. Also they have enlisted popular tools for DDOS attacks with their impact, resources and type of attack.

In [3], the paper proposed IP spoofing attack using proxy server. The communication between the attacker ,disguised as some other's actual IP address let say A, and the actual IP address is done via two or more proxy servers. The attacker sends SYN request to A's address and A sends SYN together with ACK to attacker without waiting for the ACK reply from attacker. This continues and A comes in the overflow state where it cannot reply to any more external connection request. The attacker disguised its IP address as A and then sends connection request (SYN) to target or victim address say B.B then recognizes the SYN packet received as the one sent by A so that B can send ACK back and sends a new SYN to A. But A cannot communicate with external any more .So attacker sends ACK to B as A's address. Hence an inappropriate connection is made between attacker and victim B,and B thinks that it is connected with A.Now,attacker can illegally accesses B's system.

In [4] this paper the author describes IP spoofing attacks and the proposed methods currently available to detect or prevent them. This work was followed by the "Hop-Count Filtering"

(HCF) technique proposed by Wang et al to detect IP spoofing. Their algorithm followed by basing on the idea that although an attacker may be able to spoof the source IP address, but the attacker cannot spoof the number of hops that a packet traverses while reaching the destination. Therefore, the algorithm first learns the IP to Hop Count (HC) mapping and stores the mapping in an IP2HC table [5]. Once a packet arrives, it is compared with the HC which is already stored for this IP, and if match is not found packet is discarded.

3. DDoS ATTACKS AND ITS EFECTS

Denial-of-Service attack is an attempt that makes the network resource and machine unavailable to the intended users. The attacks occur when the services is blocked by another user intentionally. This type of attack doesn't cause any damage to the data but it does not provide the required resource .DDoS attack is a mass of compromised systems, which attacks a single target that causes denial-of –service for the users in targeted system. As shown in Figure 1, DDoS attacks consist of following components:

1. Real Attacker or Masters
2. Zombie hosts that generate packets.
3. Target host or Victim.

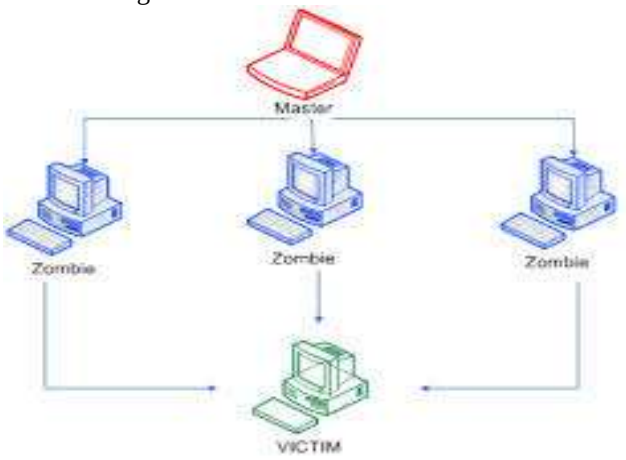


Figure 1: DDoS attack

As we know Denial of Service and Distributed Denial of Service attacks are methods which are commonly used by hackers to disrupt network services and to the corporate environments. Hackers use 'session hijacking' as a method to illegally capture sessions after a successful authentication of user with a server. By this the attacker gets access to confidential information and makes attack to the server system by using user's identity and thus his own gets hidden.

3.1. TCP SYN Flood attack

In the TCP handshake mechanism, to establish a connection between two parties there must be an agreement between them. Such an agreement is not possible, if there is no TCP client in actual existence or is a spoofed IP non-requesting client. In a TCP SYN flood attack, the attacking clients send a series of TCP requests where TCP flags are set to SYN,which are actually coming from spoofed IP addresses, tries to trick server to believe that they are asking for legitimate connections. The target server allocates corresponding buffers to each of these SYN requests and

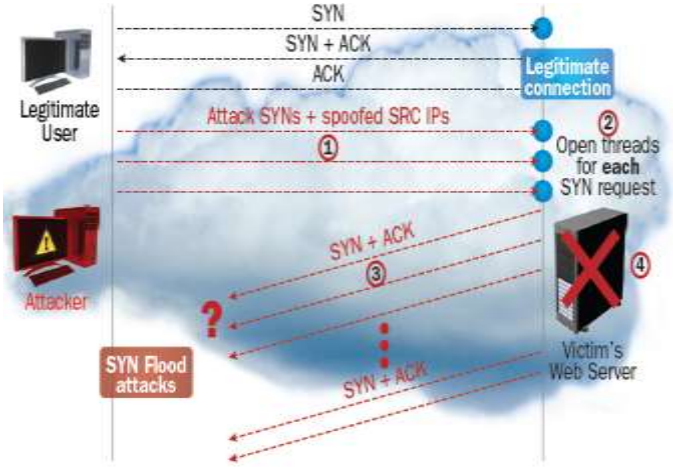


Figure 2: TCP SYN flood attack

prepares for a connection. The acknowledgement of those connection requests are sent by sending a SYN-ACK reply back to the requesting clients but the acknowledgement packet is never received to the server because of the spoofed client's IP addresses or the clients are unavailable or unable to respond back. The server attempts to resend its SYN-ACK request acknowledgement packets multiple times before requesting time-out resorts by forcing the server to maintain its open threads and buffers for corresponding original connection requests. The main cause of denial-of-service condition is that the rate of seeking of new connection request is made more than flushing out of pending open requests by sever due to time-out.

3.2. Impact

Systems may not be able to provide TCP-based services anymore to the community of Internet while under attack and also for sometime after the attack start ceasing. During attack, the service itself will not be harmed, but the ability to provide that service gets affected. There are more chances of exhaustion of system's memory, crash, or be inoperative in some cases.

3.3. Detecting an Attack

In spoofing the user of the attacked server system may not be able to notice any abnormality since the IP-spoofed connection requests may not load the system noticeably, though the system is still able to establish outgoing connections. The problem will most likely be noticed by client systems attempting to access one of the services on the victim system.Hence, to verify that this attack is occurring, the state of the server system's network traffic must be monitored regularly.

3.4. Solution

With the current IP protocol technology, yet there has been no generally accepted solution to this problem. However, one can take measures to reduce the entering of number of IP-spoofed packets into and out of the network. So till now the best method is to install a filtering router that put restriction on the

 ISSN: 2321 - 8169
861 - 865

input of your external interface (known as an input filter) by denying a packet through, if its source address comes from your internal network. Also, you can restrict the outgoing packets having different source address from that of your internal network to prevent source IP spoofing attack from originating.

Outside attackers can be prevented from sending packets to you pretending to be from your internal network by combining these two filters. By this, packets generating within your network can also be prevented which pretends to be from outside of your network. Hence Internet service providers should install these filters in your routers.

4. METHODOLOGY

In this paper we are performing an experimental analysis of DDoS attack by creating an application which is a similar to shopping portal on which attack is shown. Particularly the SYN-flood type of attack is demonstrated in this paper by hiding the attacker's identity and attack is monitored using resource monitor of the server's system.

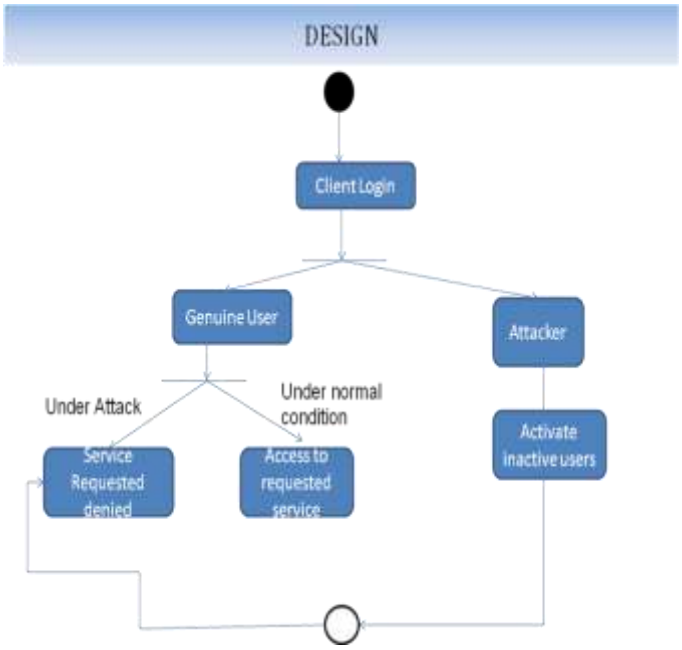


Figure 3: State chart under attack and under without attack.

To demonstrate the attack an application has been made which is similar to shopping portal using C#.net in visual studio10.We are using Mysql server for database management. The computer with Windows 7 Ultimate OS with internet information service manager (IIS) enabled is being used.

First of all connect all the computers in network. One server will install itself and make itself ready for client server communication by enabling the IIS manager of the system. The IIS manager has to be enabled to set up a machine as a server and creating the host of the network. It also shows the directories available in the root directory. Following are the key elements of this experiment as shown in above figure:

4.1. Client login

There are probably two users: one is genuine client & other is attacker. The client gets logged in. The administrator creates account for the clients by providing username & passwords to them. This privilege is provided to administrator only. By logging in one can view other user's username & passwords which is in encrypted form & various permission types which are allowed by the administrator. The encryption algorithm used for encrypting password is Triple Data encryption & standard (DES) algorithm. Client will login and start accessing web service provided by server. It is under normal condition that is before attack.

4.2. Database

There are mainly four tables which are of concern in database. Only administrator has privilege to access and make modification in database. This entire table has been created using SQL commands.

Items: - All information regarding an item /product under a particular category is stored in this table. Like, name, brand, quantity, description, cost etc.

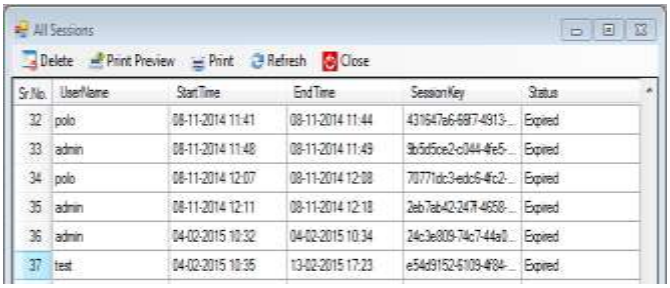
ItemGroup: This specifies in which category the items are stored.Eg Mobiles, Laptops,TV etc. Without any ItemGroup no items can be made.

Users: With this new user accounts can be created by providing username & passwords.

Session: In this the information regarding sessions of users like username, start time & end time, status whether active or inactive etc are visible. Administrator can delete unwanted entries if he wants.

4.3. Session before attack

Let us take a case, as shown in below screenshot the 'test' named user of Sr no 37 is inactive when viewed in session table.



Sr.No.	UserName	StartTime	EndTime	SessionKey	Status
32	polo	08-11-2014 11:41	08-11-2014 11:44	43164f7e6-69f7-4913-...	Expired
33	admin	08-11-2014 11:48	08-11-2014 11:49	9b5d5ce2-c044-4fe5-...	Expired
34	polo	08-11-2014 12:07	08-11-2014 12:08	70771dc3-edc6-4fc2-...	Expired
35	admin	08-11-2014 12:11	08-11-2014 12:18	2eb7ab42-24f7-4658-...	Expired
36	admin	04-02-2015 10:32	04-02-2015 10:34	24c3e809-74c7-44a0...	Expired
37	test	04-02-2015 10:35	13-02-2015 17:23	e54d9152-5109-4f84-...	Expired

Fig 4: Snapshot of session before attack

Below shows the CPU utilization in server side. We can see the graph is moderate

 ISSN: 2321 - 8169
861 - 865

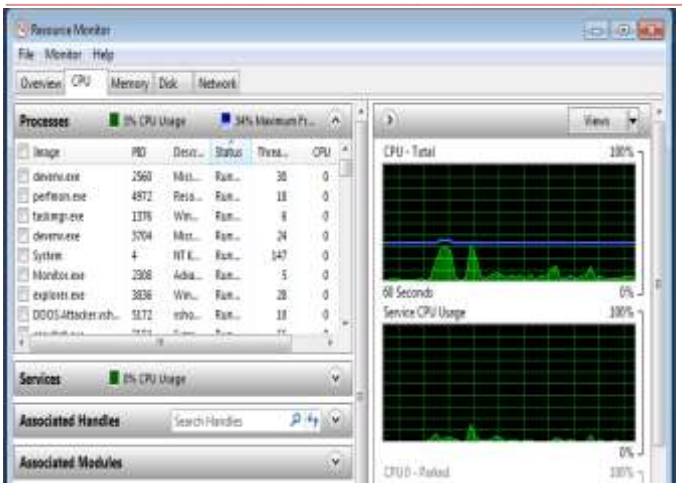


Fig 5 Resource monitor showing CPU utilization before attack

4.4. Attacker login

Attacker logins the portal as a normal client. The attacker algorithm is designed in such a way that he is able to fetch the session table where he gets details of some of the users which have accounts. The attacker has various options of attack like, he can deactivate/activate the active/inactive users, place orders, apply SYN-flood etc. And all this he can do by hiding its own identity .When administrator gets logged in he won't be able to see the active attackers account as logged in session table.

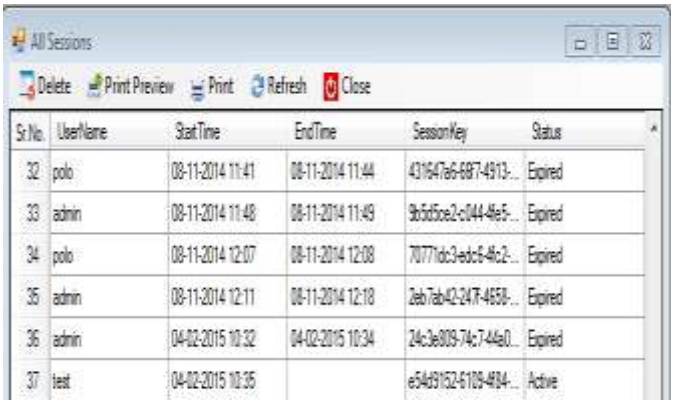


Fig 6: Snapshot of session after attack

In above case attacker has activated the inactive 'test' user.With 'test' attacker can apply SYN flood attack and the actual test user won't be able to access web services under attack.

4.5. Resource monitor

After applying SYN-flood the CPU utilization gets increased and after a certain level it becomes difficult to users to get web service access. Unless and until the IIS manager restart itself the client cannot access the web service. Following shows the CPU utilization after attack.

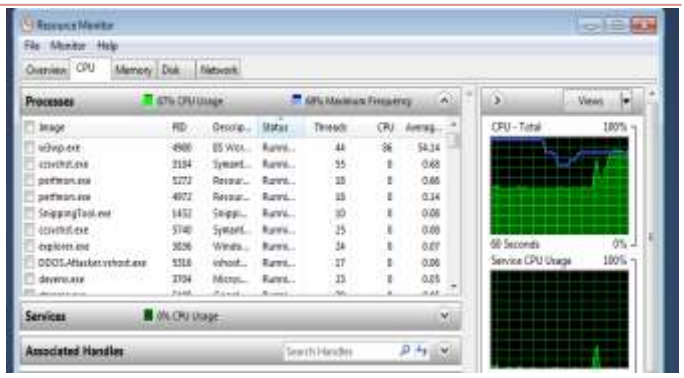


Fig 7: Resource monitors showing CPU utilization after attack

Following table depicts the overall CPU utilization on the server side which helps in analyzing the effect with and without attack.

Parameter	With Attack	W/O Attack
CPU Usage (%)	87	3

Table1: CPU usage evaluation

5. DEFENSE MECHANISMS

Following are some prevention techniques suggested which can be used to defend server from such attacks. Such techniques though not necessarily helps in identifying source generating spoofed addresses but may help in blocking them hence preventing server system from getting affected before any major harm occurring.

1. An algorithm can be developed or utility which will keep running all the time like crawler program on server side which will monitor network traffic and all the properties of clients such as IP, MAC, Request size, frequency of requests, etc. By which you can be evaluating CPU usage, requirements & time taken to process requests made onto server. Under these parameters if algorithm suggests any suspicious activity(sudden change in network traffic), it will be blocked & will clear all such request from application pool.
2. A database can be maintained of all available Bogon IPs which are used for ICMP attacks. If any request comes from those Bogon IPs, system will show alert or prompt the server administrator & it'll also add all those IPs & Mac Address into Blacklist.

6. CONCLUSION

The developed approach has been used for simulation-based evaluation of computer network security and analyzing the network security policy's efficiency and effectiveness against DDoS attacks. It is undeniable that DDoS attacks have become a menace in today's cyber security context. The attacks targeted individuals and companies such as Yahoo, Visa and Amazon. Cyber attacks are getting more sophisticated and large scale cyber attacks can bring down the Internet infrastructure of nations. We have shown DDoS attack successfully with the

help of identity spoofing and achieved our objectives. A formal paradigm for modeling and simulation of a broad spectrum of DDoS attacks is proposed.

REFERENCES

[1] Lin Jingna, "An Analysis on DOS Attack and Defense Technology", 7th International Conference on Computer Science & Education (ICCSE 2012) July 14-17, 2012. Melbourne, Australia.

[2] Arun raj kumar,S.Selvakumar "Distributed Denial of service threat in collaborative environment- A survey on DDOS tools and Traceback mechanism," IEEE International Advance Computing Conference,2009

[3] Young-Hyun Chang, Kyung-Bae Yoon, Dea-Woo Park, " A Study on the IP Spoofing Attack through Proxy Server and Defence Thereof", Information Science and Applications (ICISA), 2013 International Conference.

[4] Ayman Mukaddam, Imad Elhajj, Ayman Kayssi, Ali Chehab, "IP Spoofing Detection Using Modified Hop Count", 2014 IEEE 28th International Conference on Advanced Information Networking and Applications.

[5] Saman Taghavi Zargar,James Joshi,David Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", IEEE communications surveys & tutorials, vol. 15, no. 4, fourth quarter 2013.

[6] Diana Jeba Jingle, Elijah Blessing Rajsingh, "DDDOST: Distributed Detection of DOS Attack Using Timers in Wireless Broadband Networks", IEEE- Fourth International Conference on Advanced Computing, ICoAC 2012MIT, Anna University, Chennai. December 13-15, 2012.

[7] Liang Hu, Xiaoming Bi, "Research of DDoS Attack Mechanism and Its Defense Frame", Computer Research and Development (ICCRD), 2011 3rd International Conference.

[8] Jianpeng Zhao,Shize Guo,Kangfeng Zheng,Xinxin Niu, Yao Jiang, "An Active Defense Model for Web Accessing Dos Attacks",Information Theory and Information Security (ICITIS), 20410 IEEE International Conference.

[9] Fang-Yie Leu, and Zhi-Yang Li, "Detecting DoS and DDoS Attacks by using an Intrusion Detection and Remote Prevention System", 2009 Fifth International Conference on InformationAssurance and Security.

[10] Wei Chen, Dit-Yan Yeung, "Defending Against TCP SYN flooding Attacks Under Different Types of IP Spoofing", Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, 2006. ICN/ICONS/MCL 2006. International Conference.

[11] Kashan Samad, Ejaz Ahmed, Riaz A. Shaikh, Ahmad Ali Iqbal, "Analysis of DDoS attacksd and defense mechanisms", Technical Exposition 2005, IEEEP Student Symposium, Karachi, Pakistan, Feb, 2005.

[12] Lawan A. Mohammed and Biju Issac, "DoS Attacks and Defense Mechanisms in Wireless Networks", Mobile Technology, Applications and Systems, 2005 2nd International Conference.

[13] Stephen M. Specht, Ruby B. Lee, "Distributed Denial of Service Taxonomies of Attacks, Tools and Countermeasures", Princeton University Department of Electrical Engineering Technical Report CE-L2003-03, May 2003.

[14] Konstantinos Meintanis, Brian Bedingfield, Hyoseon Kim, "The Detection & Defense of DDoS Attack",University of Texas A&M College Station, TX, 77843.

[15] Preeti, Yogesh Chaba, Yudhvir Singh, "Review of Detection and Prevention Policies for Distributed Denial of Service Attack in MANET",Proceedings of 2nd National Conference on Challenges & Opportunities in Information Technology (COIT-2008)RIMT-IET, Mandi Gobindgarh. March 29, 2008