International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 12 | Dec-2017 www.irjet.net p-ISSN: 2395-0072

INTERNETS MANAGE COMMUNICATION PROCEDURE AND PROTECTION THAT CRASH ON SERVERS.

Ms. S. Archana varshini[1], Ms. A. Shivashankari[2],Mrs. R. Lakshmi[3]

[1] *Research Scholar, Dept of Computer Science and Applications, D.K.M. College for Women (Autonomous), Vellore, Tamilnadu, India.*
[2] *Head of the Department, Dept of Computer Science and Applications, D.K.M. College for Women (Autonomous), Vellore, Tamilnadu, India.*
[3] *Assistant Professor, Dept of Computer Science and Applications, D.K.M. College for Women (Autonomous), Vellore, Tamilnadu, India*.

Abstract-*The Internet Control Message Protocol (ICMP) is a under protocol in the Internet protocol suite. It is used by network devices, together with routers, to send error communication and outfitted information. There are special types of Cyber Security Attacks that are based on ICMP protocols. Protocols like ICMP are very comparable, which may guide security managers to think they may have same crash on fatality computer unit systems or servers. It is used by network devices, including routers, to send error announcement and outfitted information. We explore impact of different ICMP protocol based security attacks on two popular member of staff serving at table systems namely Microsoft's window Server use Ping Flood Attack and Apple's Mac Server OS use Smurf Attack organization on same hardware platform, and compare their performance under different types of ICMP based security attacks.*

Key Words*: *Internet protocol suite, DDoS Security Attacks, ICMP Based Cyber Attacks, Mac Server OS, Windows Server OS

1.INTRODUCTION

DoS attacks are recognized to crash many servers and operating systems. So much work has been done on different operating systems with DDoS attacks, but the companies are still not able to correct all problems that have been observed. In a denial of service(DoS) attacker attempt to make a network resource that is engaged to its proposed users, such as indefinitely delay or suspend services of a host connected to the internet. Denial-of-Service attack consumes a fatality computer resources such as network bandwidth, processor, memory etc. In a Denial-of-Service (DoS) attack, a single computer may attack a single computer or server, where as in a Distributed Denial of Service (DDoS) attack, many computers (Botnets) may attack a single computer. User use two very similar types (in terms of type of packets used) of ICMP based security attacks commonly known as PING flood attack and SMURF attack. We also test impact of these attacks on two different popular server OS namely, Windows Server ands Apple's Mac OS X Server LION on same hardware platform i.e. Apple's Mac Pro platform.

1.1 Ping flood attack

A ping flood is a attack where the denial-of-service (DoS) attack the attacker suppress the fatality with ICMP "echo request" (ping) packets. This is most effective by using the flood option of ping which sends ICMP packets as fast as possible without waiting for replies. Most execution of ping require the user to be privileged in order to specify the flood option. It is most successful if the attacker has more bandwidth than the fatality (for instance an attacker with a DSL line and the fatality on a dial-up modem). The aggressor hope that the fatality will respond with ICMP protocol with the "echo reply" packets, thus it consume both incoming bandwidth and the outcoming bandwidth. If the target system is slow,and it is possible to consume enough of its CPU cycles for a user to notice a significant brake. A flood ping can also be used as a pinpointing for network packet loss and throughput issues.

There is however a way to make this attack feasible even in today's environment. It is due to the broadcast mechanism build into IPv4. It is confirmed that a packet send to an Internet Protocol address containing all 1s in the host part of the address is meant to be processed by every host in the network. This means that one can send an echo request packet to a network's broadcast address and have all hosts in the network reply to it. When spoofing the origin address the attacker uses a valid address of the fatality, and has all hosts on the network that receive the broadcasted echo request reply to it. Using this technique the attacks strength gets improved by the resources (network bandwidth and CPU time of the zombie network that is used to undertake this attack), making the attack much more serious.

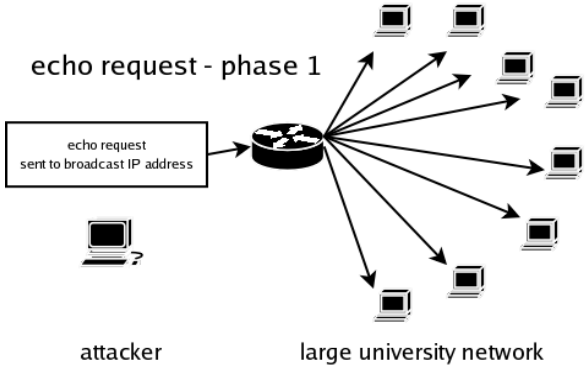

Fig1: ping flood attack

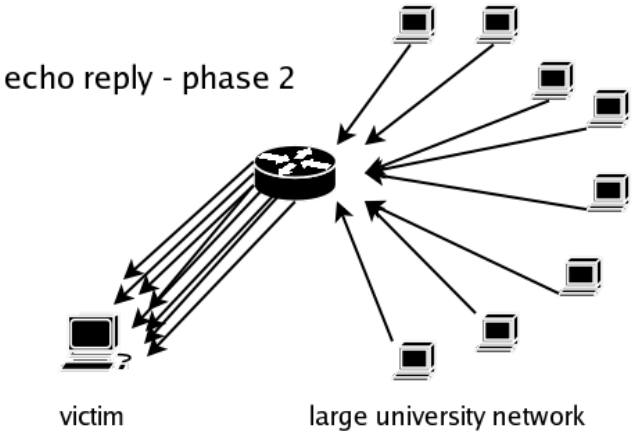

Fig2: ping flood attack

1.2.Experimental Set Up

In this experiment, simulated attack traffic is sent to the fatality server from multiple networks .In the process of evaluating the impact of attack traffic, user measured the processor utilization, memory utilization and HTTP transactions for different loads of attack traffic ranging from 100 Mbps to 1 Gbps over a gigabit Ethernet link connected to the victim computer.

The PING flood and SMURF attacks were simulated using the experimental set up. The fatality server is an Apple Mac Pro, Two 2.4 GHz Quad- Core Intel Xeon E5620 "Westmere" processors server, 8 logical processor and 12 GB RAM. As mentioned earlier, Windows Server Standard Operating System and Apple server platform to Mac OS X SERVER LION 10.7.5 (11G63) have been installed in the fatality server. We compared the performance of two servers in terms of their ability to handle legitimate HTTP connections in the presence of different ICMP protocol based attack traffic. In these experiments, the only protection mechanism that was active on the server platform was default firewall in both operating systems.

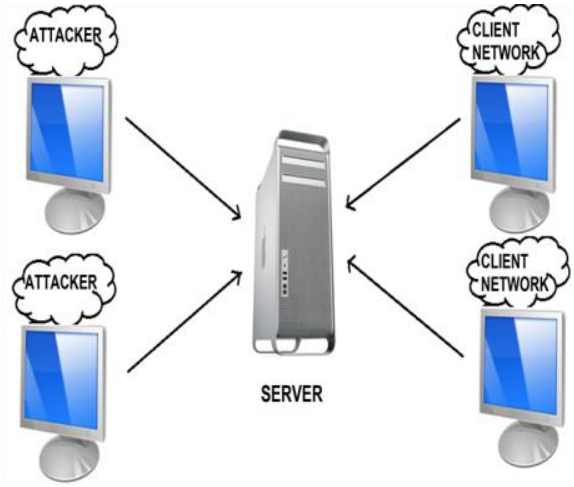

Fig3: experimental set up

1.3. Performance evolution

User test Apple server with Windows OS and Mac OS in four scenario under Ping flood attack and Smurf attack. Four evaluation scenarios are given below:

1) Ping attack on Windows Server OS on Apple server platform.

2) Ping attack on Mac OS on Apple server platform.

3) Smurf attack on Windows Server OS on Apple server platform.

4) Ping attack on Mac OS on Apple server platform.

2. Smurf attack

Smurf attack is situated under the network layer, Distributed denial-of-service (DDoS) attack, named after the DoS .Smurf malware that enables it execution. Smurf attacks are some what similar to ping floods, as both are carried out by sending a slew of ICMP Echo request packets. It is similar to the regular ping flood, however, Smurf is an extension attack vector that boosts its spoil the potential by exploiting characteristics of broadcast networks.

In a normal scenario, station A sends an ICMP protocol Echo (ping) request to station B, trigger an automatic response. The time it takes for a response to arrive is used as a measure of the virtual distance between the two stations. In an Internet Protocol broadcast network, an ping request is sent to every station, prompting a response from each of the recipients. With Smurf attacks, the attacker take advantage of this function to enlarge their attack traffic.

A Smurf attack scenario can be broken down as follows:

1. Smurf malware is used to generate a fake Echo request containing a spoofed source IP, which is actually the target server address.

2. The request is sent to an intermediate IP broadcast network.
3. The request is transmitted to all of the network hosts on the network.
4. Each host sends an ICMP response to the spoofed source address.
5. With enough ICMP responses forwarded, the target server is brought down.

The amplification factor of the Smurf attack correlates to the number of the stations on the interface network. For instance, an Internet Protocol broadcast network with 500 stations will produce 500 responses for each fake Echo requests. Normally, each of the confide is of the same size as the original ping request.

It should be noted that, during the attack, the service on the interface network is likely to be dishonored. In addition to showing good internet residency, this should encourage operators to prevent their networks from being unwitting Smurf attack participants.

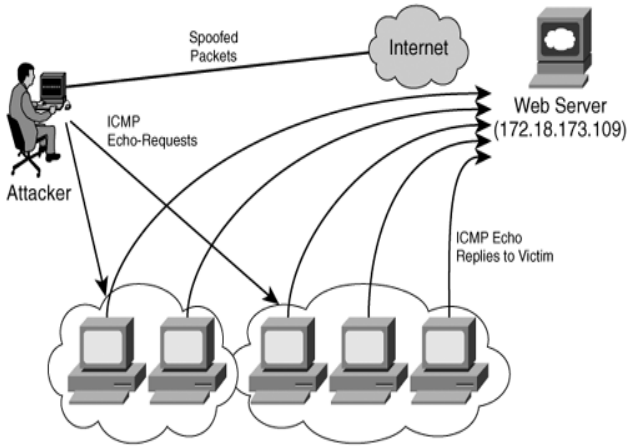

Fig4: smurf attack

3. Ping Attack on Windows Server OS on Apple Server Platform

In this scenario-1, user used the Windows Server OS on the Apple's server hardware platform. In order to analyze the effectiveness of an attack on the server, we found the maximum number of HTTP connections that can be establish on the server without the presence of attack traffic (baseline presentation), and then this results were compared with the results obtained in presence of the attack traffic.

In the beginning, the legal HTTP connections were established with the server in the absence of attack traffic, and then the replicated attack traffic was introduced in the network and intensity was measured. In order to estimate the impact of the ICMP protocol attack based traffic, the number of HTTP connections that the server could handle was recorded for various amount of attack traffic ranging from 100 Mbps to 1 Gbps. The baseline presentation of the server with no attack traffic was calculated to HTTP connections 6000per second. After baseline HTTP connections were established, replicated attack traffic was introduce in the range of 100 Mbps to 1 Gbps to the network. Traffic intensity was calculated in the steps of 100 Mbps. When the PING flood attack traffic was introduced and the baseline presentation of 6000 HTTP connections of the Windows server was maintained up to 600 Mbps of PING flood attack traffic. However, as the PING flood was improved beyond 600 Mbps, the server's baseline presentation was found to reject. The traffic attack that attain 700 Mbps, the rest number of HTTP connections get rejected to 4950 HTTP connections. At 800 Mbps of attack traffic the legal connections rejected to 350 only. Finally at senior PING flood concentration there is greater than 800 Mbps, and there is no legal connections could be established with the server.

Ping Attack on Mac OS on Apple Server Platform

For this scenario-2, we used the Apple's native MAC OS for the same Apple's server hardware platform. Comparatively, the Mac OS results were found to be different from that of Windows Server for the same hardware platform. Baseline performance could be maintained till 500 Mbps of the PING flood. A significant decline in the number of legitimate connections was found at 600 Mbps supporting only 50 legitimate connections under Ping attack. This kind of significant decline in the legitimate connections was found to be at 800 Mbps for Windows Server OS on Apple's hardware server platform. Inferring from the performance data, it showed that the Microsoft's Windows Server was performing better than Apple's Mac OS on its native Apple server hardware platform under Ping flood attack. In the scenarios 1and2 user examine the PING flood attack was based on the ICMP Echo request protocol. A very parallel protocol, namely the ICMP Echo reply protocol that is used in the Smurf security attack. The Smurf attack is based on security attack which is used to evaluate performance of two different server systems from Microsoft Inc and Apple Inc which is based on the next two situation.

Smurf Attack on Windows OS on Apple Server Platform

The Smurf flood attack was used to evaluate Windows Server OS on the same server hardware platform from Apple Inc. A drastic change was observed in Microsoft's Windows server performance under the Smurf flood attack compared to its previous performance under PING flood attack. The scenario explain, the baseline server performance of the number of legal connections destroy sharply as the Smurf attack traffic that increased beyond 100 Mbps. All legitimate client connections were lost at 150 Mbps of Smurf attack traffic, which is a relatively low attack bandwidth compared to 1000 Mbps or 1 Gbps being common these days. No

legitimate client connections could be established with the Microsoft's server OS running on the same hardware platform from Apple Inform Smurf traffic higher than 150 Mbps. This seemed quite unusual in the beginning knowing the fact that the server hardware deployed 8 core processors but the whole server system became unresponsive under relatively small volume of Smurf attack traffic of 150 Mbps. Further analysis of the core utilization showed that one of the core maxed out and other cores didn't share the excess load of the Smurf flood. It was not clear if it was due to the inability of the Window's server OS in handling the Smurf flood or was it due to the inability of the Apple's hardware platform in sharing the excess load.

In one of the literatures issued by Apple Inc, Apple gave a statement saying "It's not possible to split a single thread across multiple cores, although a single core may run multiple threads at the same time. This is one reason that you may sometimes see uneven load distributions across the available cores on your computer".

Smurf Attack on Mac OS on Apple Server Platform

User use native Mac OS on the same Apple's server hardware platform. A Smurf attack on Mac OS produced relatively improved resilience of the server compared to the crashing of Windows Server at 150 Mbps of the smurf attack load. Compared with Windows OS, Mac OS was able to sustain the Smurf attack till 300 Mbps by supporting the baseline performance. When the attack traffic increased, the number of legitimate connections started declining, and all legitimated connections were completely lost after the attack traffic increased beyond 500 Mbps

Mac OS on Apple's server hardware platform shows higher survivability compared to that for Windows Server OS on Apple's server hardware platform.

Comparing performance

The important effects to differentiate the performance of different servers under different types of ICMP protocol attacks to obtain a better picture of security provided by these leading server platforms. Comparative performance is for two server OS under two different types of ICMP protocols based attacks.

Under Ping attack, the Microsoft's Windows Server OS on Apple's server hardware performs better than Mac LION OS on its own native Apple server hardware. It is found that for the Microsoft's Windows OS, the number of legitimate connections start declining from its baseline of 6000 connections for attack traffic higher than 600 Mbps. The Hardware platform, and the number of legal connections starts from its baseline performance of 6000 connections when the Ping flood intensity exceeds 300 Mbps. Under Smurf attacks, the Microsoft's Windows server OS on MAC hardware platform is found to crash at relatively low Smurf attack intensity of 150 Mbps. The Smurf attack, and the Apple's MAC LION OS performs much better on the same Apple's Mac Pro hardware platform. The MAC OS lost all legitimate connections but at much higher attack traffic i.e. 600 Mbps. comparatively, under Smurf attack

3. CONCLUSIONS

The different server operating systems perform differently under different types of ICMP based ping flood attacks. Windows Server is one of the most popular server used today, hence even though Apple server platform has its own operating system, it is common to use Windows Server operating system on Apple Server hardware platform. It is shown in this we eximine, the Microsoft's Windows Server OS performed better in term of survivability (number of legitimate connections supported under attack) compared to Apple's Server OS under Ping based ICMP attack traffic., under the Smurf attack that based on ICMP protocol attack, the Window's Server OS crashed at a relatively low Smurf traffic of 150 Mbps. It also dropped all legal connections somewhat at higher Smurf attack traffic intensity. The results presented in this paper show that the built-in protection mechanism of Windows Server is not effective on its own against a SMURF flood attack. we wind up that both server OS need to deploy more efficient protection mechanisms especially against ICMP based Cyber attacks without depending on external security devices.

REFERENCES

[1] Kumar, S. and Gade, R. (2015) Windows 2008 vs. Windows 2003: Evaluation of Microsoft's Windows Servers under Cyber Attacks. Journal of Information Security.

[2] Kumar, S., Valdez, R. and Gomez, O. (2006) Survivability Evaluation of Wireless Sensor Networks under DDoS Attack. International Conference on Networking.
https://doi.org/10.1109/ICNICONSMCL.2006.205

[3] Kumar, S. (2005) Impact of Distributed Denial of Service (DDoS) Attack Due to ARP-Storm. The Lecture Notes in Computer Science-Book Series-LNCS-3421-Networking-ICN 2005, Part-II, Vol. 3421, 997-1002
https://doi.org/10.1007/978-3-540-31957-3_113

[4] Kumar, S. and Sekhar, R. (2011) Experimental Evaluation of Juniper Network's Netscreen-5GT Security Device against Layer4 Flood Attacks. Journal of Information Security, 2, 50-58.
https://doi.org/10.4236/jis.2011.21005

[5] Vellalacheruvu, H.K. and Kumar, S. (2011) Effectiveness of Built-In Security Protection of Microsoft's Windows Server 2003 against TCP SYN Based DDoS Attacks. Journal of Information Security, 2, 131-138.
https://doi.org/10.4236/jis.2011.23013

[6] Gade, R.S.R., Vellalacheruvu, H. and Kumar, S. (2010) Performance of Windows XP, Windows Vista and Apple's Leopard Systems under a DDoS Attack. International Conference on Digital Society (ICDS'10).

[7] Surisetty, S. and Kumar, S. (2012) Microsoft's Windows7 vs. Apple's Snow Leopard: An Experimental Evaluation of Resilience against Distributed Denial of Service (DDoS) Attacks. IEEE Security and Privacy, 10, 60-64.

[8] Baez Jr., R. and Kumar, S. (2014) Apple's Lion vs. Microsoft's Windows 7: Comparing Built-In Protection against ICMP Flood Attacks. Journal of Information Security, 5, 123-135.
https://doi.org/10.4236/jis.2014.53012

[9] Sundar, K. and Kumar, S. (2016) BlueScreen of Death Observed for the Microsoft's Server 2012 R2 under Denial of Service Attacks. Journal of Information Security, 7, 225-231.
https://doi.org/10.4236/jis.2016.74018

[10] Surisetty, S. and Kumar, S. (2010) Is Apple's iMac Leopard Operating System Secure under ARP-Based Flooding Attacks? Second International Conference on Internet Monitoring and Protection (ICIMP 2010).
https://doi.org/10.1109/ICIMP.2010.30

[11] Kumar, S. and Surishetty, S. (2011) Apple's Leopard versus Microsoft's Windows XP: Experimental Evaluation of Apple's Leopard Operating System with Windows XP-SP2 under Distributed Denial of Service Security Attacks. Information Security Journal: A Global Perspective, 20, 163-172.

[12] Aishwarya, R. and Malliga, S. (2014) Intrusion Detection System—An Efficient Way to Thwart against Dos/DDoS Attack in the Cloud Environment. International Conference on Recent Trends in Information Technology, Chennai, 10-12 April 2014, 1-6.

[13] Kumar, S. (2007) Smurf-Based Distributed Denial of Service (DDoS) Attack Amplification in Internet. 2nd International Conference on Internet Monitoring and Protection (ICIMP), San Jose, 1-5 July 2007, 25.

BIOGRAPHIES

Ms. S. Archana Varshini
Research Scholar, Dept of Computer Science and Applications, D.K.M. College for Women (Autonomous), Vellore, Tamilnadu.

Ms. A. Sivasankari
Head of the Department, Dept of Computer Science and Applications, D.K.M. College for Women (Autonomous), Vellore, Tamilnadu.

Mrs. R. Lakshmi
Assistant Professor, Dept of Computer Science and Applications, D.K.M. College for Women (Autonomous), Vellore, Tamilnadu.