Scientific Research Publishing

Journal of Information Security, 2017, 8, 274-283
http://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Do ICMP Security Attacks Have Same Impact on Servers?

Ganesh Reddy Gunnam, Sanjeev Kumar*

Department of Electrical and Computer Engineering, The University of Texas-RGV, Edinburg, USA
Email: *sjkumar1@ieee.org

How to cite this paper: Gunnam, G.R. and Kumar, S. (2017) Do ICMP Security Attacks Have Same Impact on Servers? *Journal of Information Security*, **8**, 274-283.
https://doi.org/10.4236/jis.2017.83018

Received: May 30, 2017
Accepted: July 22, 2017
Published: July 25, 2017

Abstract

There are different types of Cyber Security Attacks that are based on ICMP protocols. Many ICMP protocols are very similar, which may lead security managers to think they may have same impact on victim computer systems or servers. In this paper, we investigate impact of different ICMP based security attacks on two popular server systems namely Microsoft's Windows Server and Apple's Mac Server OS running on same hardware platform, and compare their performance under different types of ICMP based security attacks.

Keywords

DDoS Security Attacks, ICMP Based Cyber Attacks, Mac Server OS, Windows Server OS

1. Introduction

The Distributed Denial of Service (DDoS) attacks are increasing day by day. These DDoS attacks are known to crash many servers and operating systems. So much work has been done on different operating systems with DDoS attacks [1]-[12], but the companies are still not able to correct all problems that have been observed. In computing, a denial of service(DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

Denial of Service attack consumes a victim computer's 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.

In this paper, we 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 2012 R2 and Apple's Mac OS X Server LION on same hardware platform *i.e.* Apple's Mac Pro platform.

1.1. Ping Flood Attack

Ping Flood Attack is one of the oldest known network attacks, and its aim is to saturate the network with ICMP (Internet Control Message Protocol) traffic. ICMP Ping is used to verify the end-to-end internet path operation, where ICMP Echo request packet is sent to the target and an ICMP Echo Reply packet is expected to confirm communication between sender and receiver [6].

A router, or a host, uses an ICMP echo request (ping) message to test a destination's reachability. A computer system that receives an ICMP echo request message will respond to it by sending an ICMP echo reply message back to the sender (**Figure 1**). Using this, an ICMP echo request and reply messages together can test the reachability of a computer on a network [13]. The ICMP echo request and reply messages are identified by the value of the type field in the ICMP message format [14]. If the value of type field is equal to 8, it becomes echo request, if the value of type field is equal to 0, it becomes an echo reply [13].

These Ping based DDoS attacks are flood of a large number of ping messages sent to target are known to be quite damaging to the availability of the web-based services. The Ping attack can exhaust the target server's bandwidth and computing resources [14]. The victim computer continues receiving a Ping message that generates an ICMP echo reply message sent to the source address of the Echo Request.

1.2. Smurf Attack

A more sophisticated version of a DDoS attack is commonly known as a SMURF attack. A SMURF attack utilizes massive number of ICMP packets of spoofed source Internet Protocol (IP) addresses targeting the victim server's IP address

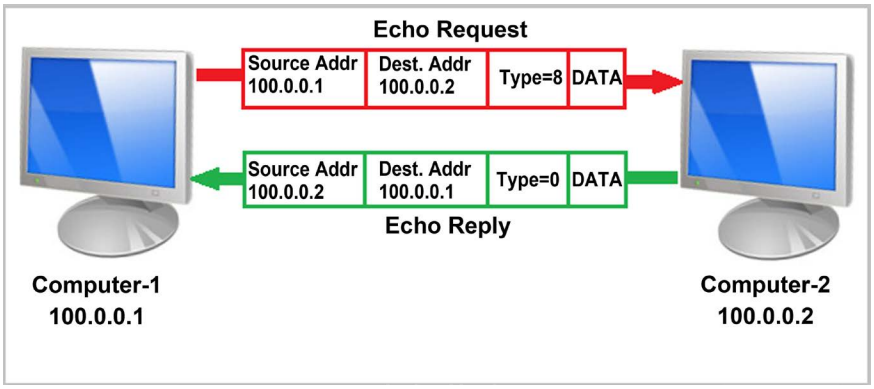

Figure 1. Ping Utility.

(Figure 2). This is achieved by altering the Echo Request sent to the botnet using an IP broadcast address [13] [15]. The larger the Botnet is the faster and the bigger is the flood of Echo reply messages [16]. The increase of traffic reduces the target server's ability to respond, and can quickly cause a complete denial of service [5] [6].

In this attack both the ICMP echo request and ICMP echo reply messages are used. While the perpetrator sends ICMP echo request messages to an unprotected broadcast domain for amplifying the attack, the victim computer actually receives amplified attack traffic that comprises mainly of ICMP echo reply messages. If the broadcast domain has N number of computers, then for each ICMP echo request broadcasted in such a domain will generate N number of ICMP echo reply messages that are sent to the victim's server, due to the spoofed source address in the ICMP echo request messages [13].

2. Experimental Set Up

In this experiment, simulated attack traffic is sent to the victim server from multiple networks (Figure 3). In the process of evaluating the impact of attack traffic, we 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 [1] [2].

The PING and SMURF attacks were simulated using the experimental set up shown in Figure 3. The victim 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 [17] [18]. As mentioned earlier, Windows Server 2012 R2 Standard Operating System and Apple server platform to Mac OS X SERVER LION 10.7.5 (11G63) have been installed in the victim server. We compared the performance of two servers in terms of their ability to handle legitimate HTTP connections in

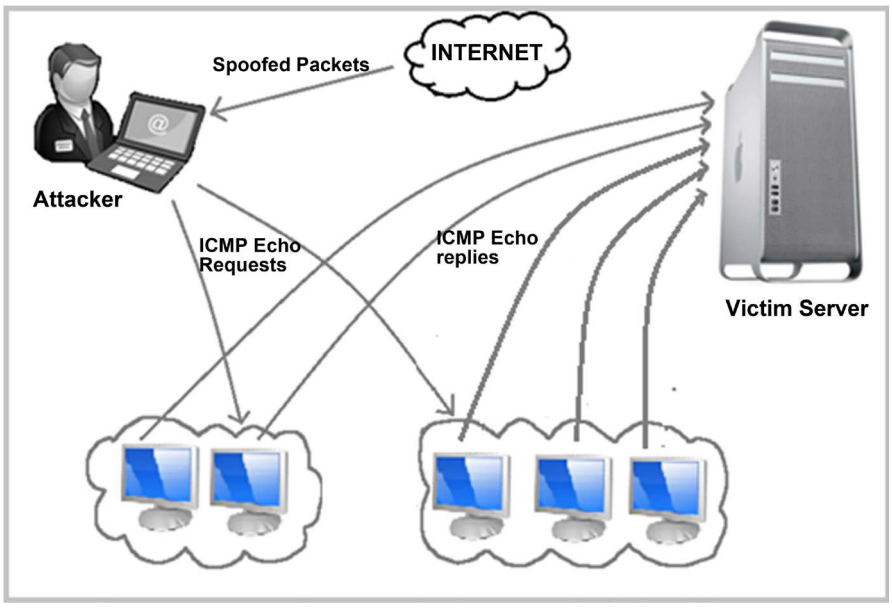

Figure 2. SMURF Attack.

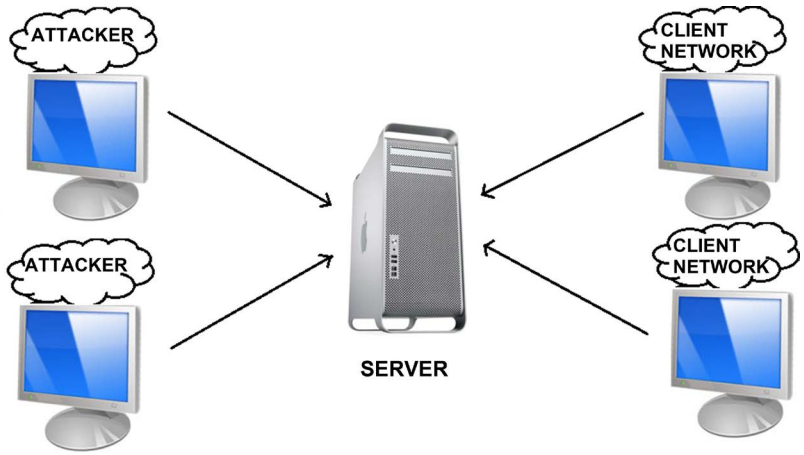

Figure 3. Experimental Set Up.

the presence of different ICMP based attack traffic. In these experiments, the only protection mechanism that was active on the server platform was default firewall in both operating systems.

3. Performance Evaluation

We test Apple server with Windows OS and Mac OS in four scenarios under Ping 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.

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

In this scenario-1, we 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 performance), and then this results were compared with the results obtained in presence of the attack traffic.

In the beginning, the legitimate HTTP connections were established with the server in the absence of attack traffic, and then the simulated attack traffic was introduced in the network and intensity was measured. In order to evaluate the impact of the ICMP based attack 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 performance of the server with no attack traffic was measured to be 6000 HTTP connections per second. After baseline HTTP connections were established, simulated attack traffic was introduced in the range of 100 Mbps to 1 Gbps to the network. Traffic intensity was measured in the steps of 100 Mbps.

When the PING attack traffic was introduced as shown in Figure 4, the base-

line performance of 6000 HTTP connections of the Windows server was maintained up to 600 Mbps of PING attack traffic. However, as the PING flood was increased beyond 600 Mbps, the server's baseline performance was found to decline. When the attack traffic reached 700 Mbps, the number of HTTP connections declined to 4950 HTTP connections. At 800 Mbps of attack traffic the legitimate connections declined to 350 only. Finally at higher PING flood intensity greater than 800 Mbps, no legitimate connections could be established with the server (Figure 4).

3.2. 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 2012 R2 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 (Figure 5). This kind of significant decline in the legitimate connections was found to be at 800 Mbps for Windows Server 2012 R2 OS on Apple's hardware server platform. Inferring from the performance data, it showed that the Microsoft's Windows Server 2012 R2 was performing better than Apple's Mac OS on its native Apple

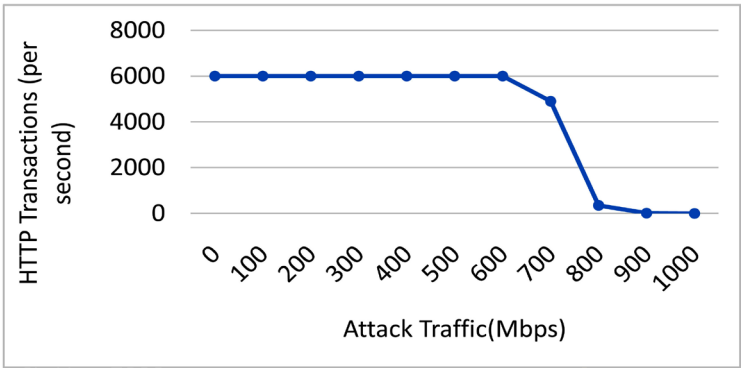

Figure 4. HTTP Connection Establishment under PING attack (scenario-1: Windows Server 2012 R2 on Apple server platform).

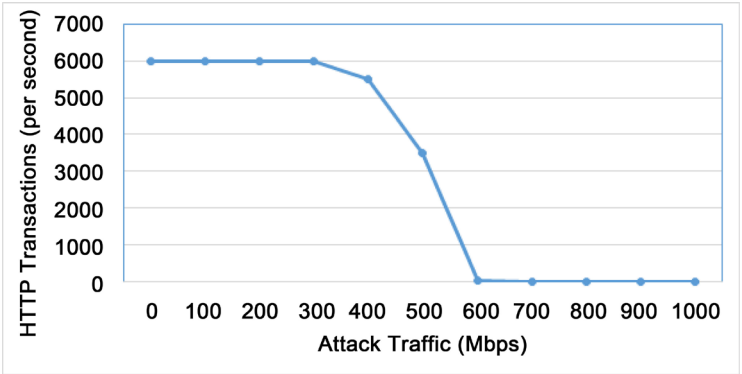

Figure 5. HTTP Transactions under PING flood attack (scenario-2: Mac Server OS on Apple's hardware server platform).

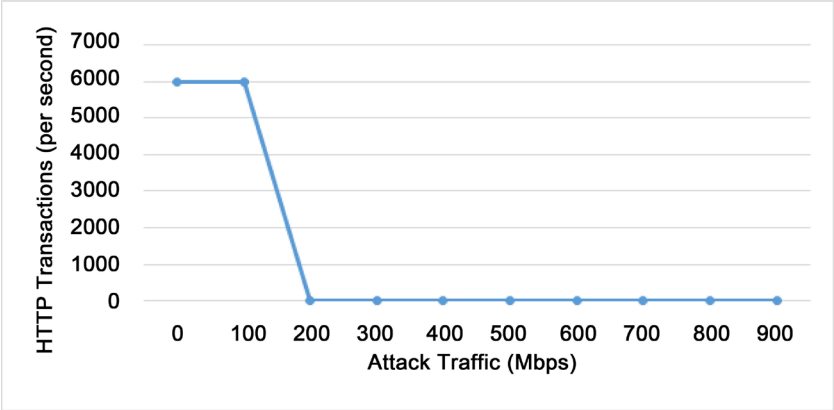

Figure 6. Legitimate connections under SMURF attack (scenario-3: Windows Server 2012 R2 on Apple server platform).

server hardware platform under Ping flood attack.

PING flood attack in the scenarios 1 & 2 above was based on the ICMP Echo request protocol. A very similar protocol, namely the ICMP Echo reply protocol is used in the Smurf security attack. In next two scenarios, Smurf based security attack was used to evaluate performance of two different server systems from Microsoft Inc and Apple Inc.

3.3. Smurf Attack on Windows OS on Apple Server Platform

In scenario-3, the Smurf flood attack was used to evaluate Windows Server OS 2012 R2 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. In this scenario, the baseline server performance of the number of legitimate connections fell sharply as the Smurf attack traffic 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 Inc. (Figure 6) for 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 [19], 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".

3.4. Smurf Attack on Mac OS on Apple Server Platform

In this scenario-4, we used 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 2012 R2 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 (Figure 7).

4. Compairing Performance

It is important to compare the performance of different servers under different types of ICMP attacks to obtain a better picture of protection provided by these leading server platforms. Comparative performance is shown in Figure 8 for two server OS under two different types of ICMP based attacks.

Under Ping attack, the Microsoft's Windows Server OS 2012 R2 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. However, for Mac OS on the same Mac hardware platform, the number of legitimate connections starts declining from its baseline 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. However, under the Smurf attack, 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 traffic, Mac OS on Apple's server hardware platform shows higher survivability compared to that for Windows Server OS 2012 R2 on

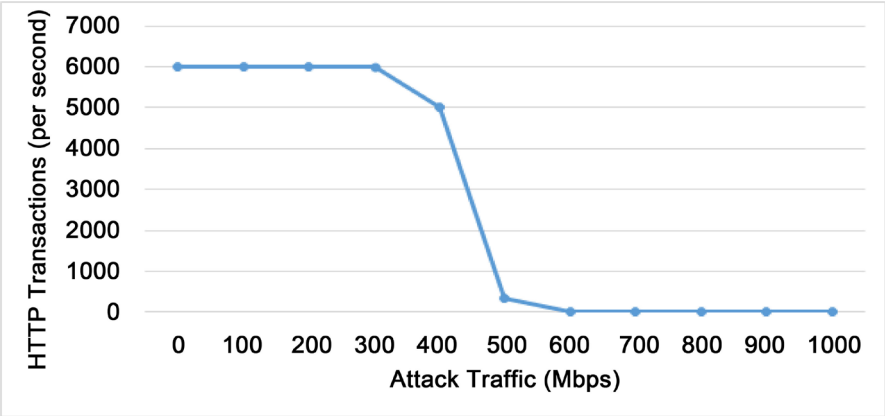

Figure 7. HTTP Transactions under SMURF attack (Scenario 4: Mac Server OS on Apple server platform).

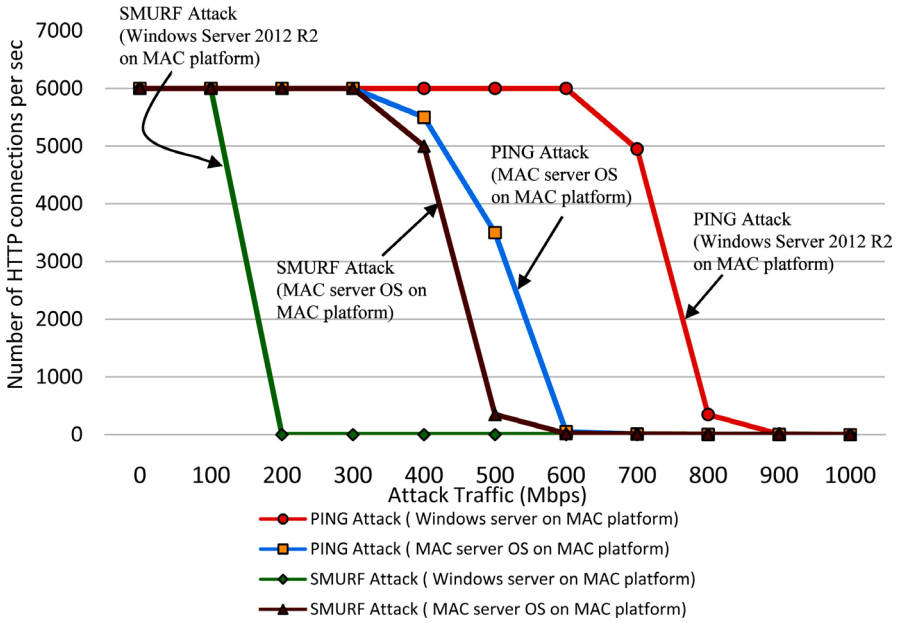

Figure 8. Comparison of legitimate HTTP Connections supported by different configurations.

Apple's server hardware platform.

5. Conclusion

It is observed that different server operating systems perform differently under different types of ICMP based flood attacks. Windows Server 2012 R2 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 2012 R2 operating system on Apple Server hardware platform. It is shown in this paper, the Microsoft's Windows Server OS performed better in term of survivability (number of legitimate connections supported under attack) when compared with that of Apple's Server OS under Ping based ICMP attack traffic. However, under Smurf based ICMP attack, the Window's Server OS crashed at a relatively low Smurf traffic of 150 Mbps. For the same Smurf attack the Apple's Server OS survived under the same scenario of 150 Mbps. However, it also dropped all legitimate connections rather at higher Smurf traffic intensity. The results presented in this paper show that the built-in protection mechanism of Windows Server 2012 R2 is not effective on its own against a SMURF flood attack. We conclude that both server OS need to deploy more efficient protection mechanisms especially against ICMP based Cyber attacks without depending on external security devices.

Acknowledgements

My sincere thanks to Arturo Gomez and Ronald Palomares for reviewing this paper. The support for this research is providing in part by the US National Science Foundation under Grant No. 0421585 and Houston Endowment Chair in Science, Math and Technology Fellowship.

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. 2*nd International Conference on Internet Monitoring and Protection* (*ICIMP*), San Jose, 1-5 July 2007, 25.

[14] Kumar, S. (2006) PING Attack—How Bad Is It. *Computers & Security*, **25**, 332-337.

[15] Smurf Attack. http://en.wikipedia.org/wiki/Smurf_attack

[16] Ferguson, P. and Senie, D. (2000) Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing. RFC 2827, BCP 38.

[17] Mac Pro (2010) Technical Specifications. http://support.apple.com/kb/SP589?locale=en_US

[18] Solid-State Drive Replacement Instructions for Mac Pro. http://manuals.info.apple.com/MANUALS/1000/MA1548/en_US/Mac_Pro_SSD_DIY.pdf

[19] Apple Statement on Core Distribution. http://support.apple.com/en-us/HT201838