Journal of Information Security, 2015, 6, 155-160
Published Online April 2015 in SciRes. http://www.scirp.org/journal/jis
http://dx.doi.org/10.4236/jis.2015.62016

Scientific Research Publishing

Evaluation of Microsoft Windows Servers 2008 & 2003 against Cyber Attacks

Sanjeev Kumar, Senior Member, Raja Sekhar Reddy Gade

Department of Electrical Engineering, The University of Texas-Pan American, Edinburg, TX, USA
Email: sjk@utpa.edu

Received 17 March 2015; accepted 27 April 2015; published 28 April 2015

Abstract

Distributed Denial of Service (DDoS) is known to compromise availability of Information Systems today. Widely deployed Microsoft's Windows 2003 & 2008 servers provide some built-in protection against common Distributed Denial of Service (DDoS) attacks, such as TCP/SYN attack. In this paper, we evaluate the performance of built-in protection capabilities of Windows servers 2003 & 2008 against a special case of TCP/SYN based DDoS attack. Based on our measurements, it was found that the built-in security features which are available by default on Microsoft's Windows servers were not sufficient in defending against the TCP/SYN attacks even at low intensity attack traffic. Under TCP/SYN attack traffic, the Microsoft 2003 server was found to crash due to processor resource exhaustion, whereas the 2008 server was found to crash due to its memory resource depletion even at low intensity attack traffic.

Keywords

Cyber Warfare, Distributed Denial of Service Attacks, TCP/SYN Flood, Processor Resource Exhaustion, Memory Resource Exhaustion

1. Introduction

Cyber warfare is making headlines very frequently worldwide. Distributed Denial of Service (DDoS) is one of the common tools being used in today's Cyber warfare and to compromise legitimate online transactions. Recent target of such coordinated attacks have been Twitter, Facebook, YouTube, Sony PlayStation network, Master Card etc. just to name few, whose websites were brought down by Distributed Denial of Service (DDoS) attacks and in some cases customers' confidential information were compromised. According to the research reports and surveys conducted by from Arbor Networks [1], thousands of DDoS attacks were happening every day and intensity of attack is increasing rapidly. In 2013, the DDoS attack intensity was found to exceed 300 Gbps,

How to cite this paper: Kumar, S., Member, S. and Gade, R.S.R. (2015) Evaluation of Microsoft Windows Servers 2008 & 2003 against Cyber Attacks. *Journal of Information Security*, **6**, 155-160. http://dx.doi.org/10.4236/jis.2015.62016

which was three times the maximum attack intensity observed in 2012. Internet is omnipresent in today's information society including health care facilities and hospitals. DDoS attacks on Internet connected health care facilities can also lead to failure of proper health care in our society [2]. Servers are the backbone of today's Internet driven data centers, and bringing down these servers can result in significant disruption of today's Cyber driven society. Furthermore, 71% of data center operators reported DDoS attacks in 2013, which was up 45% from 2012 [1]. To understand the effectiveness of security protections, in this paper, we evaluate two commonly deployed Microsoft's Windows servers, namely Windows 2003 and Windows 2008 servers, and their built-in security capabilities to protect against a common DDoS attack called TCP/SYN flood attack.

This paper is organized as follows: Section II presents a brief background on DDoS attacks, especially on TCP/SYN attack. Section III gives information about experimental setup and default systems configurations of the servers under test. Section VI presents results and discussion, and Section V is conclusion.

2. Background

DDoS attacks are increasing both in terms of frequency and attack intensity. DDoS attacks have been found to occur with increasing intensity-largest intensity was reported to be 100 Gbps in 2010 and in 2013 the largest intensity was reported to be over 300 Gbps [1]. There are different types of DDoS attacks; however, most work by flooding a large amount of illegitimate traffic towards the victim server that causes denial of service to legitimate users by consuming all of the available recourses of the victim computer such as Memory depletion, Processor exhaustion or Bandwidth consumption [2]-[6]. Some DDoS attacks can also be caused by sending small amount of traffic to exploit a given vulnerability on the victim computer/server [7].

2.1. TCP/SYN Flood Attack

A TCP/SYN flood is one of the common mechanisms used by hackers to launch DDoS attacks. This occurs when an attacker remotely uses its Botnets to send a flood of TCP/SYN packets, often with forged IP addresses towards a victim server/computer. The victim server/computer treats TCP/SYN packets like a normal connection requests, creates half-open connections, and sends back acknowledgement packets called TCP/SYN-ACK packets for every TCP/SYN packets received. The victim server waits for a response from the senders. Since the senders' IP addresses are forged, the follow up response never comes. The half-open connections created at the victim computer saturate the number of available connections that the server can make, and thus limiting the total number of legitimate connections that can be established.

For every TCP-SYN packet that is received, the victim computer allocates TCB resources before establishing a complete connection by following 3-way handshake process. Continuous flood of TCP-SYN packets lead to ever increasing allocation of TCB resources and thus resulting in exhaustion of resources of a victim computer [8] [9]. Normally TCB requires 280 Bytes and in some operating systems up-to 1300 Bytes depending on the complexity of the TCP algorithms and options used. If an attacker sends continuous flood of TCP-SYN packets with spoofed IP address then the targeted server replies to the spoofed IP with a SYN-ACK and reserves some resources for the client and waits for final ACK. For a high-load of attack traffic, in no time, the resource of the targeted victim server can be completely consumed resulting in Denial of Service for the legitimate users.

2.2. Default Inbuilt Prevention against TCP/SYN Attack

For Windows 2003 server with Service Pack2, there is a built-in security feature provided by the operating system called "Syn Attack Protect", which is enabled by default for Windows Servers 2003 with Service Packs installed. This protection reduces the amount of retransmissions of the SYN-ACKS, which also reduces the allocated memory for TCB entry resources for the incoming SYN segment until the full connection is established after completing three-way handshake process. And, this protection mechanism is activated when the Tcp Max-Half Open and Tcp Max Half Open Retried threshold levels are exceeded [10] [11]. Tcp Max Half Open is a parameter which manages the number of connections in the SYN-Received (SYN-RCVD) state before the Syn-Attack Protect protection begins to functions, and by default, this threshold is set to 500 in Windows Server Enterprise Edition. And Tcp Max Half Open Retried is a parameter which manages the number of connections in SYN-RCVD state for which one retransmission of SYN segment has to be sent, before the Syn Attack Protect begins to function. Regarding Windows 2008, it appears to be tuned by default for performance and protection,

such that modification of these registry entries doesn't provide the same performance benefits that have been observed on Windows Server 2003 [11] [12].

3. Experimental Setup

In our experiments, we launched a TCP/SYN based DDoS attack to observe the inbuilt ability of the Microsoft servers 2003 (with SP-2) and 2008 (with SP-1, which was the first release of server 2008 with service pack) to defend on its own against the TCP/SYN based network attacks. No external security systems were deployed in these experiments in order to understand inbuilt attack prevention capability these servers. Two different server platforms used in the experiments were Microsoft Windows Server 2003 with Service Pack-2 (Enterprise ×64 Bit Editions) and Microsoft Windows Server 2008 with Service Pack-1 (Enterprise × 64 Bit Editions) on Intel® Xeon® CPU E5345 @ 2.33 GHz with Memory (RAM): 8.00 GB. The Microsoft Windows servers 2003 (with SP-2) & 2008 (with SP-1) under test were configured as HTTP Servers.

4. Results and Discussions

4.1. Protection Provided by Microsoft Windows Server 2003 (with SP-2) against TCP/SYN Attack

In this case, first the legitimate HTTP traffic from different clients on Internet was sent towards the targeted server. Web Server configured on the Microsoft Windows Server 2003 (SP-2) resulted in maximum of 20,000 connections per second, in the absence of any attack traffic sent towards the server. This formed the baseline for the number of connections supported by the Windows Server 2003.

To measure the impact of the TCP/SYN attack on the Windows Server 2003, different loads of such attack traffic were sent towards the server in the range of 0 Mbps (baseline) to 10 Mbps. The impact of TCP/SYN attack was measured in terms of the processor utilization and the number of legitimate connections that could be supported in the presence of the TCP/SYN attack traffic. It was observed that the processor consumption of the Windows Server reached to 100% at 6 Mbps, which is a small amount of attack traffic compared to the server's interface speed of 1 GB. Unlike processor, memory was not completely exhausted. The memory consumption was found to be 197 Mb under 6 Mbps of attack traffic (**Figure 1**).

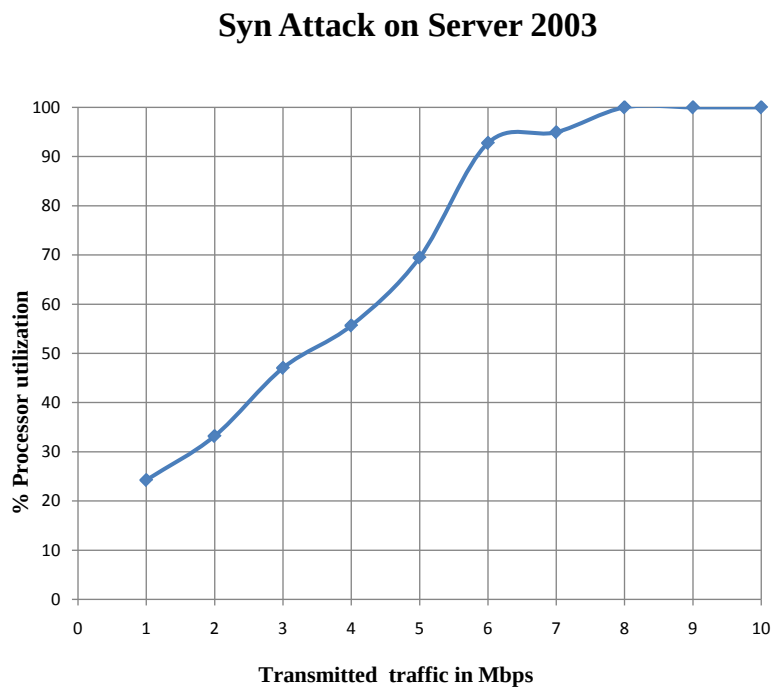

Figure 1. Processor utilization Vs TCP/SYN attack load on Microsoft Windows server 2003 service pack-2.

To evaluate impact of the TCP/SYN attack on number of legitimate connections-first, legitimate HTTP traffic is sent to Windows Server 2003 to maintain 20,000 connections per second. Thereafter, TCP/SYN attack traffic of increasing load is directed towards the Windows Server 2003. From **Figure 2**, it is observed that the number of connections which were 20,000/sec in the absence of any TCP/SYN attack (*i.e*. zero attack load which forms the baseline) continues to decline as the attack traffic increased. The number of legitimate connections continued to decline with increase in attack load, *i.e*. from a baseline of 20,000 connections/sec and eventually reached to zero connections at an attack load of 6 Mbps of TCP/SYN attack traffic.

4.2. Protection Provided by Microsoft Windows Server 2008 (SP-1) under TCP/SYN Attack

As a baseline, we first determine the maximum number of connections that the Windows Server 2008 SP-1 can provide to the legitimate users in the absence of TCP/SYN attack traffic. By sending HTTP traffic from different legitimate users to the server, it was found that Windows Server 2008 (with SP-1) could establish 25,000 Connections/Second in the absence of any TCP/SYN attack traffic.

To determine the impact of attack, different loads of TCP/SYN traffic was sent towards the Windows Server 2008. Even though the number of connections supported by the Windows 2008 Server were higher than those supported by the Windows 2003 Server, the number of connections continued to drop as the TCP/SYN traffic load increased. The number of connections/sec dropped to half of the baseline *i.e*. 12,000/sec when the TCP/SYN attack traffic load reached 3 Mbps (**Figure 3**).

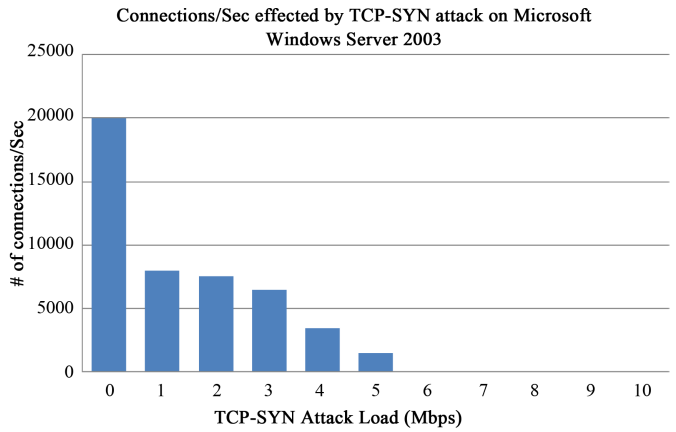

Figure 2. Number of TCP connections per second Vs TCP/SYN attack load experienced by Windows Server 2003 (with SP-2).

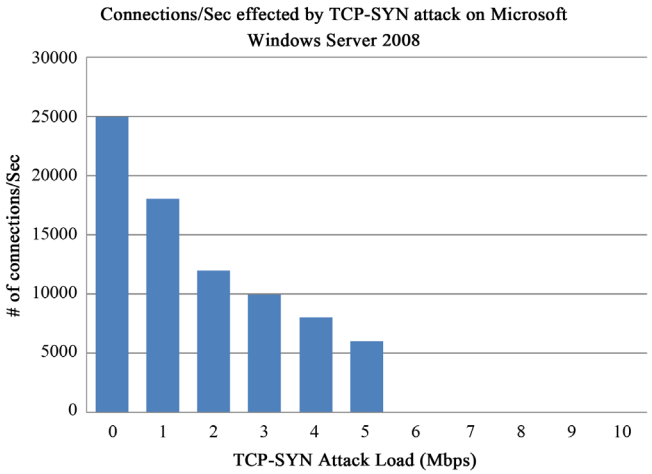

Figure 3. Number of TCP connections/sec Vs TCP/SYN attack load on Windows Server 2008 SP-1.

At 5 Mbps of TCP/SYN attack traffic load, the connections were brought down to 6000 connections/sec. Interestingly, when the load was further increased to 6 Mbps, the server was found to have crashed resulting in zero connections to legitimate users.

To understand the cause of the crash, a relatively higher load of 10 Mbps of TCP/SYN attack traffic was sent again to the Windows 2008 Server with SP-1, and it was found that Microsoft Windows Server 2008 crashed rather due to rapid depletion of the memory, whereas the processor was not consumed completely. **Figure 4** shows a snapshot of rapid memory depletion causing the Windows 2008 Server to crash in less than 60 seconds.

Comparison of two different Windows Servers under TCP/SYN attack traffic is shown in **Table 1**.

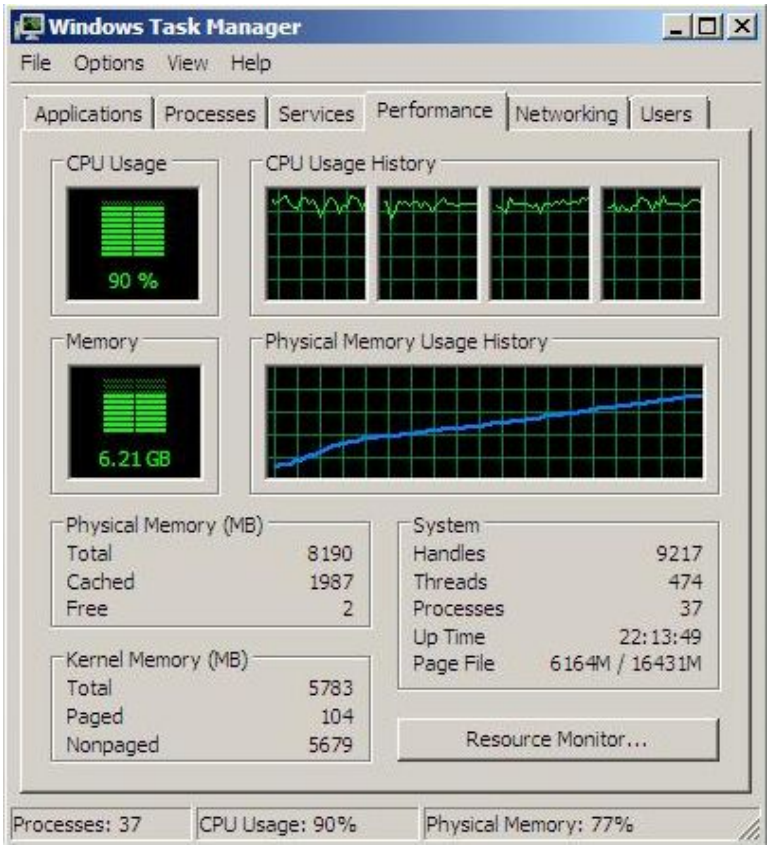

Figure 4. Snapshot of the memory depletion at 10 Mbps of TCP/SYN attack traffic on Windows 2008 server with SP-1.

Table 1. Comparison of TCP connections/sec established with Microsoft Windows 2003 and 2008 servers under presence of TCP/SYN flood of varying loads.

TCP/SYN Attack Load	Max # of legitimate TCP-Connections/Sec	
	Windows-2003	Windows-2008
No Attack (baseline)	20,000	25,000
1 Mbps	8000	18,000
2 Mbps	7500	12,000
3 Mbps	6500	10,000
4 Mbps	3500	8000
5 Mbps	1500	6000
6 Mbps	0	0

5. Conclusion

In this paper, we evaluated the security availability of Windows Servers 2003 (with SP-2) and 2008 (with SP-1) under the presence of TCP/SYN based DDoS attacks. The Windows 2008 Server was found to support more connections/sec compared to Windows 2003 server under conditions of no network attacks, nevertheless both servers rapidly lost legitimate connections as the TCP/SYN based attack traffic increased in intensity. It was discovered that Microsoft Windows Server 2003 (with SP-2) crashed due to complete processor exhaustion at relatively low flood of TCP/SYN traffic which was around 6 Mbps. The Windows Server 2008 (with SP-1) was found to crash also at 6 Mbps of TCP/SYN attack traffic however the crash was due to the memory depletion rather than the complete processor exhaustion, which resulted in zero legitimate connections for the users. The experimental evaluations presented in this paper shows that the built-in security capability of Windows servers are not sufficient to withstand TCP/SYN based DDoS attacks on their own. It is important for the server farm operators to not rely solely on the host-based, built-in protection provided by the Microsoft's Windows servers. Additional security systems such as intrusion prevention systems must be deployed strategically on the periphery of the network to allow security protection against DDoS attacks.

References

[1] Arbor Networks, Worldwide Infrastructure Security Report. http://www.arbornetworks.com/research/infrastructure-security-report

[2] Petana, E. and Kumar, S. (2011) TCP SYN Based DDoS Attack on EKG Signals Monitored by a Wireless Sensor Network. *Journal of Security and Communication Networks*, **4**, 1448-1460. http://dx.doi.org/10.1002/sec.275

[3] Kumar, S. and Petana, E. (2008) Mitigation of TCP/SYN Attacks with Microsoft's Windows XP Service Pack2 (SP2) Software. 7*th International Conference on Networking*, 2008. http://dx.doi.org/10.1109/ICN.2008.77

[4] Gade, R., Vellalacheruvu, H. and Kumar, S. (2010) Performance of Windows XP, Windows Vista and Apple's Leopard Computers under a Denial of Service Attack. 4*th International Conference on Digital Society*, St. Maarten, 10-16 February 2010. http://dx.doi.org/10.1109/ICDS.2010.39

[5] Surisetty, S. and Kumar, S. (2010) Is Apple's iMac Leopard Operating System Secure under ARP-Based Flooding Attacks? *IEEE* 4*th International Conference on Digital Society*, St. Maarten, 10-16 February 2010, 178-181.

[6] Kumar, S. and Surisetty, 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. http://dx.doi.org/10.1109/MSP.2011.147

[7] Windows 7, Vista Exposed to "Teardrop Attack". ZDNet, Sept 8, 2009.

[8] W. Eddy, RFC 4987 "TCP SYN Flooding Attacks and Common Mitigations. www.ietf.org/rfc/rfc4987.txt

[9] Transmission Control Protocol/Internet Protocol (TCP/IP) (technet.microsoft.com/en-us/library/cc759700(WS.10).asxp) © 2010 Microsoft Corporation.

[10] Tuning TCP/IP Response to Attack. technet.microsoft.com/en-us/library/cc759239(WS.10).aspx

[11] TCP/IP Registry Values for Microsoft Windows Vista and Windows Server 2008. (www.microsoft.com/downloads/details.aspx?FamilyID=12ac9780-17b5-480c-aef7-5c0bde9060b0&displaylang=en

[12] Registry Settings That Can Be Modified to Improve Network Performance. http://msdn.microsoft.com/en-us/library/ee377084(v=bts.10).aspx