Journal of Information Security, 2016, 7, 225-231
Published Online July 2016 in SciRes. http://www.scirp.org/journal/jis
http://dx.doi.org/10.4236/jis.2016.74018

Scientific Research Publishing

Blue Screen of Death Observed for Microsoft Windows Server 2012 R2 under DDoS Security Attack

Koushicaa Sundar, Sanjeev Kumar*

Department of Electrical and Computer Engineering, The University of Texas—RGV, Edinburg, Texas, USA
Email: *sj.kumar@utrgv.edu

Received 31 March 2016; accepted 4 July 2016; published 7 July 2016

Abstract

Microsoft server Operating Systems are considered to have in-built, host based security features that should provide some protection against Distributed Denial of Service (DDoS) attacks. In this paper, we presented results of experiments that were conducted to test the security capability of the latest server Operating System from Microsoft Inc., namely Windows Server 2012 R2. Experiments were designed to evaluate its in-built security features in defending against a common Distributed Denial of Service (DDoS) attack, namely the TCP-SYN based DDoS attack. Surprisingly, it was found that the Windows Server 2012 R2 OS lacked sufficient host-based protection and was found to be unable to defend against even a medium intensity3.1 Gbps-magnitude of TCP-SYN attack traffic. The server was found to crash within minutes after displaying a Blue Screen of Death (BSoD) under such security attacks.

Keywords

Network Security, Server Security, DDoS Attack, TCP SYN Flood, Blue Screen of Death

1. Introduction

Nowadays, huge and long-lasting DDoS attacks as high as 600 Gbps are being observed against organizations and are making headline news frequently [1]. DDoS attacks have far-reaching consequences and leave a lasting impact on the victim organization by affecting the trust of the customers, loss of data and loss of revenue. The attacks launched had become more and more sophisticated and vicious, such as the ransomware attack in which attackers demanded ransom to decrypt sensitive medical information which they had encrypted by exploiting an

*Corresponding author.

How to cite this paper: Sundar, K. and Kumar, S. (2016) Blue Screen of Death Observed for Microsoft Windows Server 2012 R2 under DDoS Security Attack. *Journal of Information Security*, **7**, 225-231. http://dx.doi.org/10.4236/jis.2016.74018

unpatched vulnerability in an application server [2]. It has been predicted that the occurrence of such attacks could increase in 2016 [3]. Under such circumstances, it is very crucial that organizations take a closer look at the inherent vulnerabilities and the host-based defense mechanisms available in the servers that have been deployed in their offices, and such measures would greatly decrease the chances of falling prey to attacks [4].

The inherent vulnerability due to incomplete TCP-SYN handshakes was identified as early as 1994 [5]. TCP SYN based DDoS attack is considered a common type of denial of service attacks [6] and many server platforms lack sufficient protection against this attack. Many schemes have been suggested to defend against this DDoS attack, however, not many server platforms are automatically implementing effective protections against such attacks.

The first TCP-SYN attack, also known as SYN flood attack, was reported in 1996 [7]. Since then, network system security has been improved to a great extent through the development of technologies such as Intrusion Detection and Intrusion Prevention Systems, Firewalls, Proxies and through the implementation of several strategies such as SYN cookies [8], packet filtering based on sender IP addresses, reducing the SYN-RECEIVED timer, recycling the oldest half-open Transmission Control Block (TCB), SYN cache [9] to name a few.

Most of these prevention mechanisms are used as an external mechanism (such as intrusion prevention system) to protect a server against a TCP SYN flood attack with varying results. Nevertheless, it is important for a server operating system to deploy on its platform in-built security to defend itself in the event that all the external protection mechanisms may have failed or compromised. Active research needs to be done to improve the ability of the Operating Systems to withstand and defend against DDoS attacks on its own to some extent as a part of host based defense mechanism.

Being one of the highest used server and client operating system in the world, earlier versions of Microsoft Windows operating systems have been evaluated previously [11]-[17]. Over the years, security of the server systems has improved and has become less vulnerable to attacks compared to their predecessors. There has been improvement in the protection mechanisms developed by Microsoft in the subsequent server operating system, however, more remains to be done.

2. TCP/SYN Attack

TCP, a layer-4 protocol, was implemented to ensure reliable data delivery. Hence, TCP forms an integral part of the Internet. Along with reliability, it also provides flow control and congestion control. Flow control is employed to prevent the sender from overwhelming the receiver by sending data at a rate higher than the receiver can accept. Congestion Control is used to make sure that the buffers of routers located at the core of the Internet do not overflow (**Figure 1**).

TCP ensures data reliability by creating a connection between the sender and the receiver through a three-way handshake mechanism, hence TCP is known as a connection-oriented protocol. In the first step of the three-way handshake, the sender sends a connection request by setting the SYN bit in the TCP packet to 1. The second step involves the receiver sending a SYN-ACK packet with both SYN and ACK bits set to 1 upon receiving the SYN request from the sender. In addition to sending SYN-ACK, the receiver also allocates buffers and variables for each TCP connection. In the third and final step, the sender sends an ACK packet to the receiver and allocates buffers and variables following which the connection is set up [10].

This mechanism in the TCP connection establishment that requires that the receiver (server) allocate resources before the completion of the three-way handshake is exploited in the TCP/SYN attack. To launch this

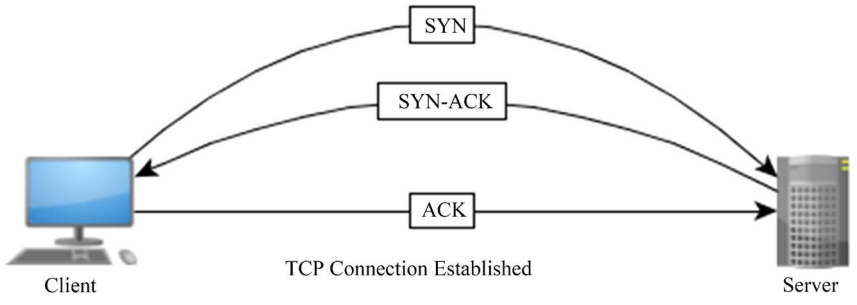

Figure 1. Legitimate three-way handshake.

attack, an attacker commands his botnets to send a volley of SYN packets to the victim. For each SYN packet the victim receives, the victim is forced to send a SYN/ACK packet and allocate resources. With increasing number of SYN requests, the server keeps on allocating resources, and this keeps the victim server too occupied to be able to handle the connection requests of legitimate users leading to a denial of service (**Figure 2**).

3. Experimental Set Up

In the experiment, simulated TCP-SYN attack traffic is sent to the victim server simultaneously from multiple networks. In order to observe the impact of the attack in an organization-like environment, legitimate or client traffic is also sent to the server simultaneously along with attack traffic.

The first TCP-SYN attack was performed using the experimental set up is shown in **Figure 3**. The victim server is a Dell Power Edge T320 tower server with Intel Xeon E5-2407 v2 quad core processor and 8 GB RAM. As mentioned earlier, Windows 2012 R2 Standard Operating System has been installed in the victim server. Since the objective of this experiment is to evaluate the inherent protection mechanism of the server Operating System, the only protection mechanism that was active on the server platform was the Windows Server 2012 R2 firewall.

4. Evaluation

In order to analyze the effect of the attack on the server, the maximum number of HTTP connections that the server can establish in the absence of attack traffic is determined (baseline performance). This result is then compared with the results obtained when the server experienced attack.

Initially, the legitimate HTTP connections were established with the server in the absence of any attack, and then the simulated attack traffic was introduced in the network and intensity was measured. In order to observe the impact of the attack traffic, the number of HTTP connections that the server could handle was recorded for different magnitudes of attack traffic ranging from 1 Gbps to 6 Gbps.

The baseline or nominal performance of the server in the absence of attack traffic was measured to be at the rate of 54,000 HTTP connections per second. In the absence of attack, the server could successfully handle all

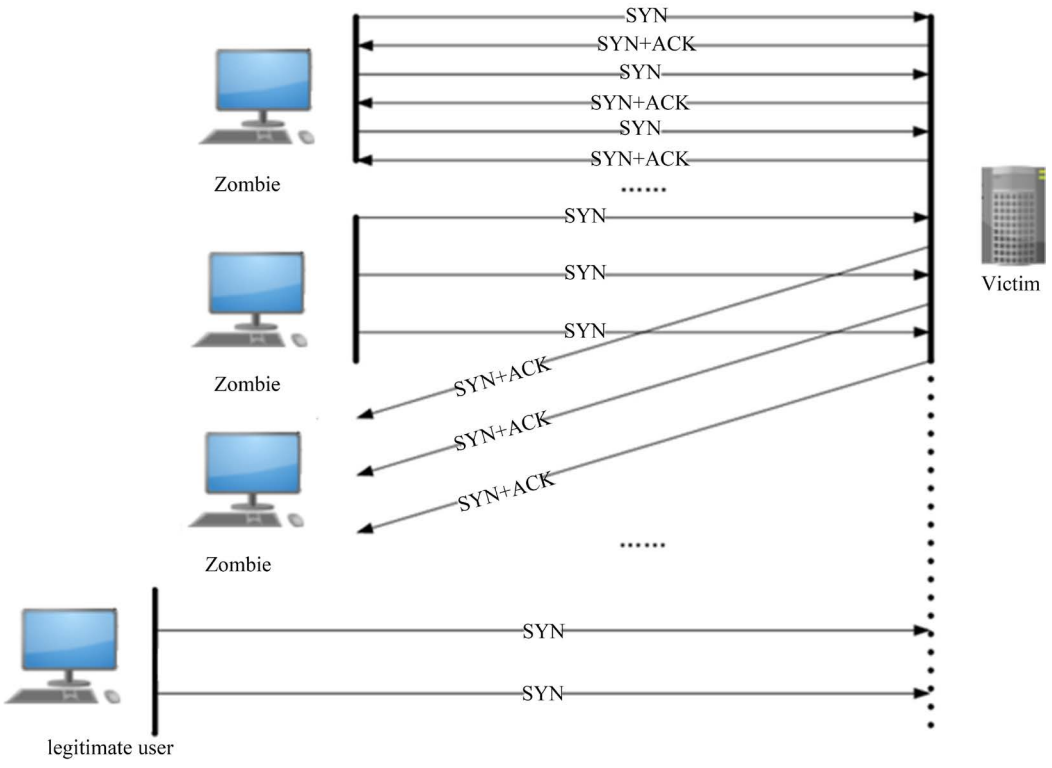

Figure 2. TCP/SYN attack.

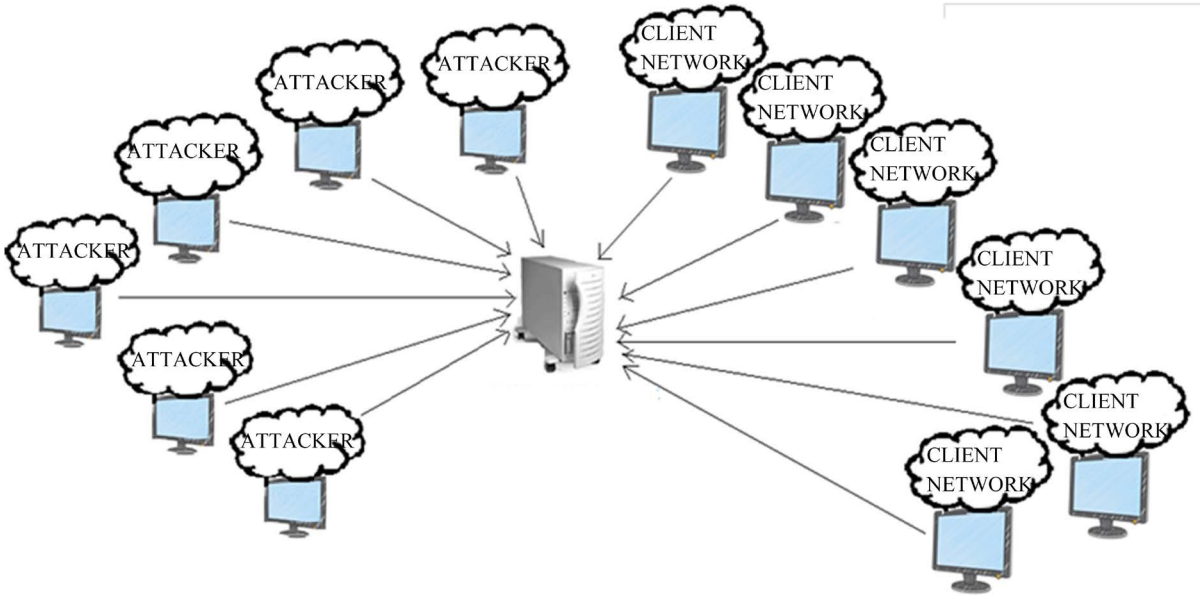

Figure 3. Experimental set up.

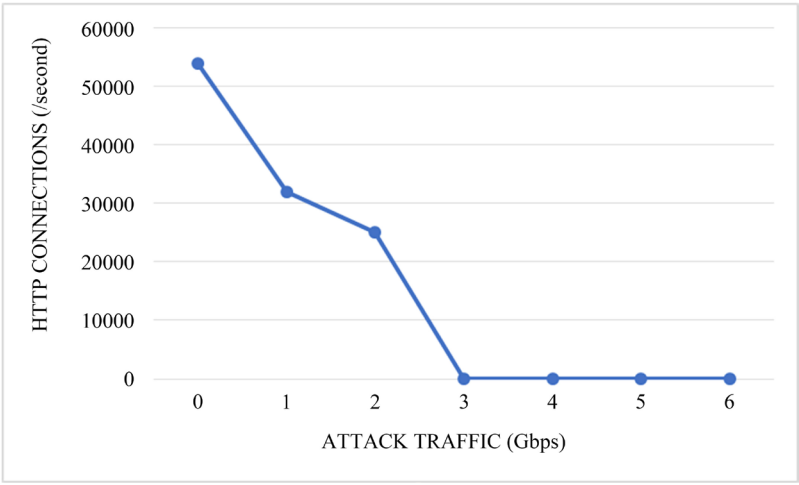

Figure 4. HTTP connection establishment for the victim server under TCP SYN attack.

the HTTP connections. Once the baseline HTTP connections were established, then simulated attack traffic was gradually introduced into the network and traffic intensity was measured.

Due to the attack traffic, the number of legitimate connections that the server could handle was observed to decrease. When the server experienced 1 Gbps of the attack traffic the HTTP connections were found to be 32,000 connections as opposed to the initial baseline value of 54,000 connections. It was observed that under the attack traffic of 2 Gbps, the number of HTTP connections further dropped to 25,000 connections per second, and for 3 Gbps of attack intensity, no HTTP connections could be established with the server.

The HTTP connections were measured under different attack traffic conditions. **Figure 4** shows the drop in the number of HTTP connections under different magnitude of attack traffic.

Table 1 displays the number of HTTP connections that the server could handle at different magnitudes of attack traffic.

It was observed that under 3.1 Gbps attack traffic, the server crashed in 3 minutes and displayed a Blue Screen of Death (BSoD) which displayed a Watchdog Violation Error (133) before restarting. **Figure 5** shows the BSoD displayed by the server.

It was further observed that as the attack traffic increased, the server took less time to crash. **Figure 6** displays

Table 1. Number of HTTP connections established by the server under SYN attack traffic.

MAGNITUDE OF ATTACK TRAFFIC	NUMBER OF HTTP CONNECTIONS (/sec)
Baseline (no attack Traffic)	54,000
1 Gbps	32,000
2 Gbps	25,000
3 Gbps	0
4 Gbps	0
5 Gbps	0
6 Gbps	0

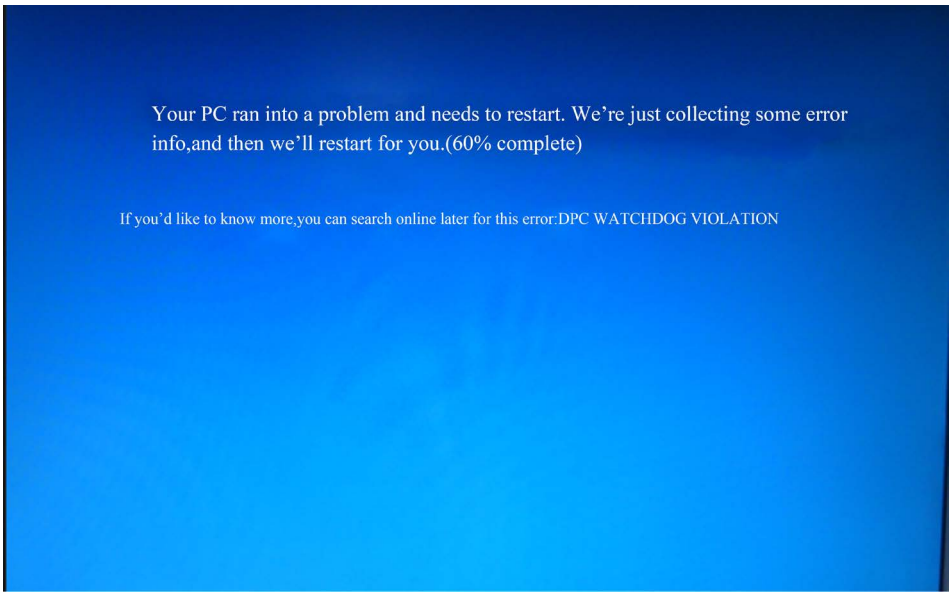

Figure 5. Blue screen of death (BSoD) displayed before the server crashed under 3.1 Gbps attack traffic.

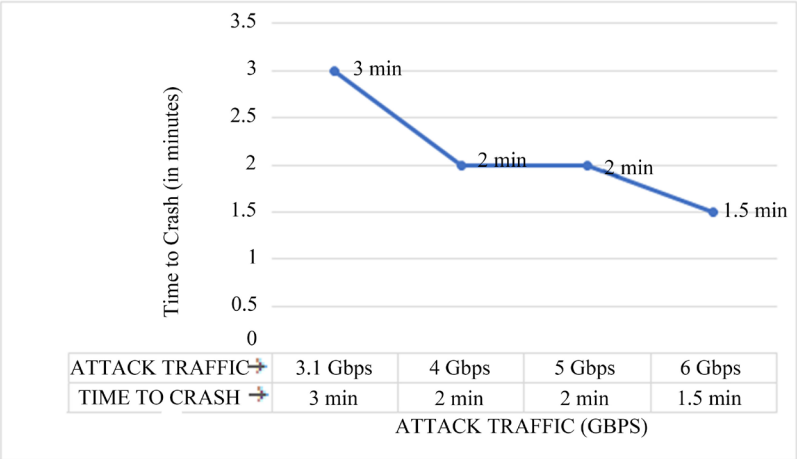

Figure 6. Duration of time the server is able to withstand the attack traffic before crashing.

the time it took for the server to crash under different attack traffic that was measured starting from 3.1 Gbps to 6 Gbps. To solve this problem, the Windows Server 2012 R2 OS was updated with the updates available from Microsoft [18]-[21] but the server continued to crash under the attack. It can be seen from **Figure 6** that the server crashed in (as little as) 1.5 minutes when it experienced a 6 Gbps of SYN attack traffic.

5. Conclusion

Windows Server 2012 R2 being one of the most used server Operating Systems, is expected to have a reasonable host based protection against security attacks including Distributed Denial of Service (DDoS) attacks. The experiments show that the inbuilt protection mechanism of Windows Server 2012 R2 is not effective enough against a common type of DDoS attack namely the TCP SYN flood attack. It is highly recommended for the network security managers worldwide to evaluate their servers' performance against a range of prescribed security attacks before their deployment in the production network.

Acknowledgements

The support for this research is provided in part by the US National Science Foundation under Grant No. 0421585.

References

[1] Khandelwal, S. (2016) 602 Gbps! This May Have Been the Largest DDoS Attack in History. The Hacker News, Jan 8. http://thehackernews.com/2016/01/biggest-ddos-attack.html

[2] Cox, J.W. (2016) Possible "Ransomware" Attack Still Crippling Some MedStar Hospitals' Computers. The Washington Post, Mar 30. https://www.washingtonpost.com/local/likely-ransomware-cyberattack-still-crippling-medstar-health-computers-at-some-hospitals/2016/03/30/a82c9fa8-f687-11e5-8b23-538270a1ca31_story.html

[3] (2015) Ransomware Attacks to Grow in 2016. Security Magazine, Nov 23. http://www.securitymagazine.com/articles/86787-ransomware-attacks-to-grow-in-2016

[4] Krishnan, R. (2016) Ransomware Attacks on Hospitals Put Patients at Risk. Apr 3. http://thehackernews.com/2016/04/hospital-ransomware.html

[5] Eddy, W. (2007) TCP SYN Flooding Attacks and Common Mitigations. Request for Comments (RFC)-4987, August. https://tools.ietf.org/html/rfc4987

[6] Zeifman, I. (2015) Q2 2015 Global DDoS Threat Landscape Report: Assaults Resemble Advanced Persistent Threats. Incapsula Blog, Bots & DDoS, Jun9. https://www.incapsula.com/blog/ddos-global-threat-landscape-report-q2-2015.html

[7] (1996) Daemon 9, Route and Infinity, Project Neptune. Phrack Magazine, Volume Seven, Issue 48, File 13 of 18, July. http://phrack.org/issues/48/13.html

[8] Bernstein, D.J. (2005) SYN Cookies. December. https://cr.yp.to/syncookies.html

[9] Lemon, J. (2002) Resisting SYN Flood DoS Attacks with a SYN Cache. BSD Conference, February.

[10] Kurose, J.F. and Ross, K.W. Computer Networking: A Top-Down Approach. 6th Edition.

[11] Kumar, S. and Gade, R.S.R. (2015) Evaluation of Microsoft Windows Servers 2008 & 2003 against Cyber Attacks. *Journal of Information Security*, **6**, 155-160.

[12] Kumar, S. and Surisetty, S. (2012) Microsoft vs. Apple: Resilience against Distributed Denial-of-Service Attacks. *IEEE Security & Privacy*, **10**, 60-64.

[13] 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.

[14] 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.

[15] Gade, R.S.R., Vellalacheruvu, H.K. 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 the Digital Society* (*ICDS* 2010), 188-191.

[16] Kumar, S. and Petana, E. (2008) Mitigation of TCP-SYN Attacks with Microsoft's Windows XP Service Pack2 (SP2) Software. *IEEE Computer Society* 7*th International Conference on Networking* (*ICN* 2008), 238-242.

[17] Kumar, S. and Petana, E. (2011) TCP SYN-Based DDoS Attack on EKG Signals Monitored via a Wireless Sensor Network. *Security and Communication Networks*, **4**, 1448-1460. http://onlinelibrary.wiley.com/doi/10.1002/sec.275/full

[18] (2012) Determining the Source of Bug Check 0x133 (DPC_WATCHDOG_VIOLATION) Errors on Windows Server 2012. MSDN blogs, Dec 7.

http://blogs.msdn.com/b/ntdebugging/archive/2012/12/07/determining-the-source-of-bug-check-0x133-dpc-watchdog-violation-errors-on-windows-server-2012.aspx

[19] (2015) Windows Stop Error 133 Occurs on Windows Server 2012. Knowledge Base Dell Support, Jun 30. http://www.dell.com/support/article/us/en/04/SLN291258/EN

[20] (2012) Knowledge Base (KB) 2789962: You Receive a "DPC_WATCHDOG_VIOLATION (133)" Stop Error Message on a Windows Server 2012-Based Computer, Article ID: 2789962, Last Review: Dec 12, Revision: 4.0. https://support.microsoft.com/en-us/kb/2789962

[21] (2015) Knowledge Base (KB) 301379: Stop Error When There's Faulty Hardware in Windows 8.1 or Windows Server 2012 R2. Article ID: 3013791, Last Review: Jul 14, Revision: 3.0. https://support.microsoft.com/en-us/kb/3013791