Journal of Information Security, 2011, 2, 113-121
doi:10.4236/jis.2011.23011 Published Online July 2011 (http://www.SciRP.org/journal/jis)

McAfee SecurityCenter Evaluation under DDoS Attack Traffic

Sirisha Surisetty, Sanjeev Kumar
Network Security Research Lab, Department of Electrical/Computer Engineering,
The University of Texas-Pan American, Edinburg, USA
E-mail: *sjk@utpa.edu*
Received February 13, 2011; *revised April* 18, 2011; *accepted May* 12, 2011

Abstract

During the Distributed Denial of Service (DDoS) attacks, computers are made to attack other computers. Newer Firewalls now days are providing prevention against such attack traffics. McAfee SecurityCenter Firewall is one of the most popular security software installed on millions of Internet connected computers worldwide. "McAfee claims that if you have installed McAfee SecurityCentre with anti-virus and antispyware and Firewall then you always have the most current security to combat the ever-evolving threats on the Internet for the duration of the subscription". In this paper, we present our findings regarding the effectiveness of McAfee SecurityCentre software against some of the popular Distributed Denial Of Service (DDoS) attacks, namely ARP Flood, Ping-flood, ICMP Land, TCP-SYN Flood and UDP Flood attacks on the computer which has McAfee SecurityCentre installed. The McAfee SecurityCentre software has an in built firewall which can be activated to control and filter the Inbound/Outbound traffic. It can also block the Ping Requests in order to stop or subside the Ping based DDoS Attacks. To test the McAfee Security Centre software, we created the corresponding attack traffic in a controlled lab environment. It was found that the McAfee Firewall software itself was incurring DoS (Denial of Service) by completely exhausting the available memory resources of the host computer during its operation to stop the external DDoS Attacks.

Keywords: Distributed Denial of Service (DDoS) Attack, McAfee Firewall, NonPaged Pool Allocs, ARP Flood, Ping-Flood, ICMP Land, TCP-SYN Flood, UDP Flood Attack

1. Introduction

Firewall is one of the most popular security software installed on millions of Internet connected computers worldwide. Today's PCs need the protection provided by a firewall to ensure the safety of both personal data, inbound and outbound traffic. Having a firewall, benefits the user and the PC by shielding them from the attacks of malicious users, would be the general thinking of a common PC user. Are these Personal Firewalls, which are provided by the most popular Antivirus companies to protect your system, safe? This is the question that we are trying to answer in this paper by evaluating the effectiveness of these personal firewalls. We know that the Firewall plays a vital role in defending against DDoS attacks. Sometimes they will cause some overhead while they are defending against the DDoS attacks. In this paper we will study the overhead, if any, caused by the McAfee SecurityCenter software firewall in defending the system against the Denial of Service attacks namely ARP Flood, Ping Flood, ICMP LAND, TCP-SYN Flood and UDP Flood attacks. We considered one attacks per layer, *i.e.*, from Layer-2 to Layer-4 in the TCP/IP suite.

"McAfee claims that it's security products use the award-winning technology and if you have installed McAfee SecurityCentre with anti-virus and anti-spyware and Firewall then you always have the most current security to combat the ever-evolving threats on the Internet for the duration of the subscription" [1]. There are different types of Distributed Denial of Service (DDoS) attacks and they exhaust resources of a victim computer differently such as processor, memory or bandwidth resources. The famous websites like e-Bay, e-Trade, Yahoo, Twitter and Facebook were also the victims of these DDoS attacks [2,3]. Recently, efforts have been made to increasingly deploy security systems such as Firewalls

and IPS (Intrusion Prevention Systems) to provide security against DDoS attacks. However, most recent DDoS attacks during July 4th, Independence Day weekend in 2009, on South Korean and US government websites convey the fact that even Firewalls and IPS, commonly deployed in the network, do not always help in defending against the DDoS Attacks [4,5]. In this July 4th, 2009 attack, the websites of a number of US and South Korean government agencies crashed and their computers experienced continuing problems since the cyber attack was launched. Not only Firewalls and IPSs the service packs released also are not able to prevent the attacks completely [6].

Some of the DDoS attacks are the Ping Flood Attack, ICMP Land Attack, TCP-SYN Attack, ARP Flood Attack and UDP Flood Attack. All of these can cause Denial of service by storming the host with the respective attack traffic. Some of them are used to bring down the host in a Local Area Network where as some can bring down a host in internet that can be a web server or Internet root servers itself [7]. To evaluate the performance of McAfee SecurityCenter's Personal Firewall against such DDoS attacks, we experimented with so called and commercially promoted, secure computer system, namely Apple's iMac with Windows XP-SP2 operating system. We also compared the performance of McAfee SecurityCenter when the iMac platform is deploying Windows XP-SP2 with that of a DELL Inspiron 530 desktop built with Vista Business and McAfee SecurityCentre with Personal Firewall and 2 GB of RAM. We consider attacks at Layer-2, Layer-3 and Layer-4 in the TCP/IP suite in this paper. The rest of the paper is organized as follows: Section 2 provides the information about experimental setup. In Section 3 we present experiments to evaluate effect of different attacks on the McAfee SecurityCenter. Section 4 is conclusion followed by Section 5 as Acknowledgment and Section 6 as references.

2. Experimental Setup

The experimental setup was used to simulate the network condition as shown in **Figure 1**. All of the DDoS attacks were simulated in controlled lab environment of Networking Research Lab of Electrical/Computer Engineering here at the University of Texas-Pan American, by making multiple computers send a barrage of corresponding attack traffic to the Victim computer up to a maximum speed of 1000 Mbps/1 Gbps. We stressed out the McAfee personal firewall installed on an Apple iMac with Windows XP-SP2 operating system at the same transmission rate but changing the load at every step starting from 10 Mbps to 100 Mbps in steps of 10 Mbps

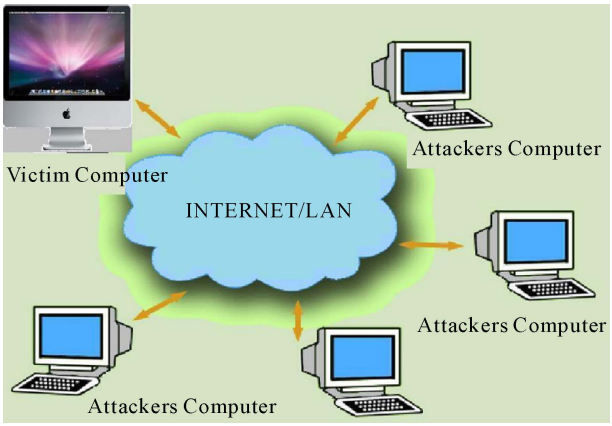

Figure 1. Distributed denial of service (DoS) attack.

and from 100 Mbps to 1 Gbps in steps of 100 Mbps. Each load is transmitted for 10 minutes duration. The victim computer is an Apple iMac with Windows XP-SP2 installed in it with McAfee SecurityCenter and also a DELL Inspiron 530 Desktop Computer with McAfee SecurityCenter.

The parameters of performance evaluation considered for this experiment were the Processor utilization and the NonPaged Pool Allocations in the main memory. NonPaged Pool allocs are those pages that can never be paged out of the system as these are Kernel functions and device drivers that in particular require real memory and should be present always for execution of a process [8,9]. During the experiment, the needed performance metric values were logged by the system under attack for analysis purposes by using some of the system activity commands. The logs were the performance counters available in the system. The Ping Flood, Smurf Attack, ICMP Land, TCP-SYN Flood, ARP Flood and UDP Flood attacks are performed on McAfee under that was installed on Windows XP and the results are as shown in Section 3.

3. Experimental Evaluation under Different DDos Attacks

In this section the background on different DDoS attacks that we consider for this experimentation are discussed and the results per each DDoS attacks are explained. The description of the results starts from the order of layers *i.e.*, from lower layer (layer-2) (ARP Attack) to higher layers (layer-4) (UDP Flood) in the TCP/IP suite.

3.1. ARP Flood Attack

Address Resolution Protocol (ARP) is used in Local Area networks to resolve IP addresses into hardware MAC addresses. It is a very basic and essential protocol

used to communicate in LAN either by gateway or by any host. The ARP request message consists of the IP address of the host, IP and hardware MAC address of the initiator who wish to communicate and broadcasts that within the LAN. All the hosts in the LAN receives the ARP request but only the host who has that IP will respond and unicast the initiator its hardware MAC (Medium Access Control) address. Also the ARP cache table of receiver host will be updated with the corresponding IP-MAC addresses for further communication with the initiator [10]. Attackers take advantage of this protocol and try to flood the end host with ARP Requests and the host ultimately ends up in replying to those requests and updating its cache table and gets busy with this task. With a flood of such requests, resource starvation usually happens on the host computer. Those resources can be either processor consumption or memory. One general way of DDoS is to storm the host with a barrage of ARP requests thereby incurring a DDoS attack on the host while being consumed in replying to all the requests it receives and exhausts the system resources. ARP-based flooding attack is a Layer-2 attack.

ARP Flood Attack on McAfee SecurityCenter

In this case the ARP flood was sent to iMac with Windows XP-SP2 operating system, with windows Firewall OFF and McAfee Personal Firewall ON. The processor utilization due to this ARP-based flooding attack is shown below in **Figure 2**. The upper line shows the maximum processor utilization, the middle line shows the average procesor utilization and the bottom line shows the minimum processor utilization of Windows XP with McAfee SecurityCenter for ARP-based flooding attack traffic. It can be observed that the average processor utilization was just 50% even for maximum attack load of 1Gbps. In this case we can say that the system with McAfee Firewall was able to sustain tha attack.

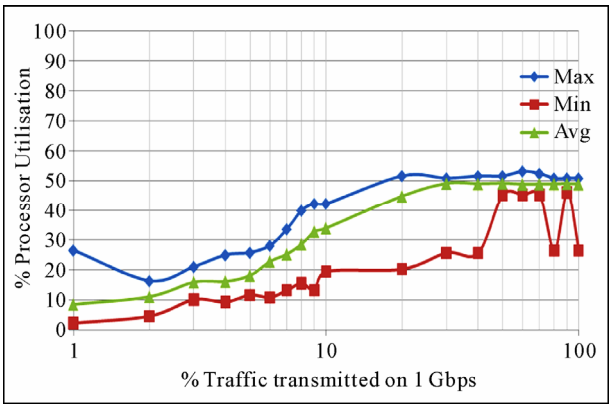

Figure 2. Processor utilization (on a logarithmic scale) of iMac deploying windows XP OS with McAfee SecurityCenter firewall under ARP attack.

3.2. Ping Flood Attack

Ping is a type of ICMP message that is used to know the reachability of a host. Based on RFC 0792 [11], ICMP Echo request must be replied with an ICMP Echo Reply message. Attackers take advantage of this protocol and try to flood the end host with Ping Requests and the host ultimately replies to those requests and hence consumes the computer resources. With a flood of such requests, resource starvation usually happens on the host computer. The attacker, generally, spoofs the source IP and sends a barrage of Ping requests to the victim computer. The victim computer incurs Denial of Service while being consumed in replying to all the requests it receives. This Ping Flood Attack is a Layer-3 attack in the TCP/IP suite. One of the earlier work shows that a simple Ping attack can make the target host busy in processing the ping requests consuming 100% of the CPU utilization [12].

Ping Flood Attack on McAfee SecurityCenter

Ping Flooding traffic is sent to the iMac deploying Windows XP-SP2 with McAfee SecurityCenter. When the attack was started the simply froze after a while giving a BSoD (Blue Screen of Death). When restarted the system displayed the message on the screen as shown in **Figures 3** and **4**. After restarting the system again 1Gbps of traffic is sent to it and again the system behaved in the same manner giving the BSoD. **Figures 5** and **6** show the Pool NonPaged bytes and Allocs for this time. The processor utilization was just 50% on an average. The default mode of McAfee firewall is to block the incoming ping requests as shown in **Figure 7** above. We have not opted for "Allow ICMP ping requests", so we assume that the ICMP ping requests are not allowed and hence system will be safe. But just after start of the attack, the system froze showing the BSoD and then it can be observed from the **Figures 5** and **6** that it has just taken 8 seconds for the system to hang up before giving the BSoD and the Pool Nonpaged Allocation have grown exponentially. After the

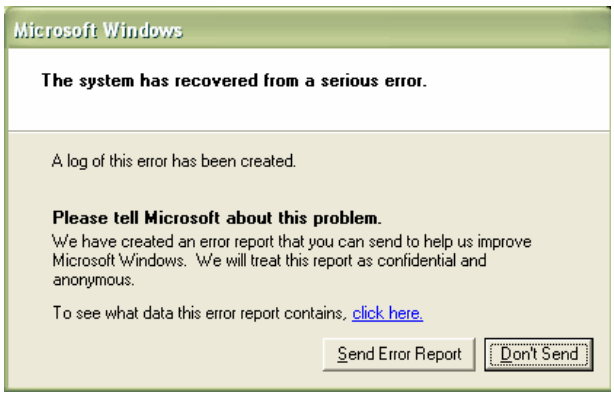

Figure 3. System error message after restarting from BSoD.

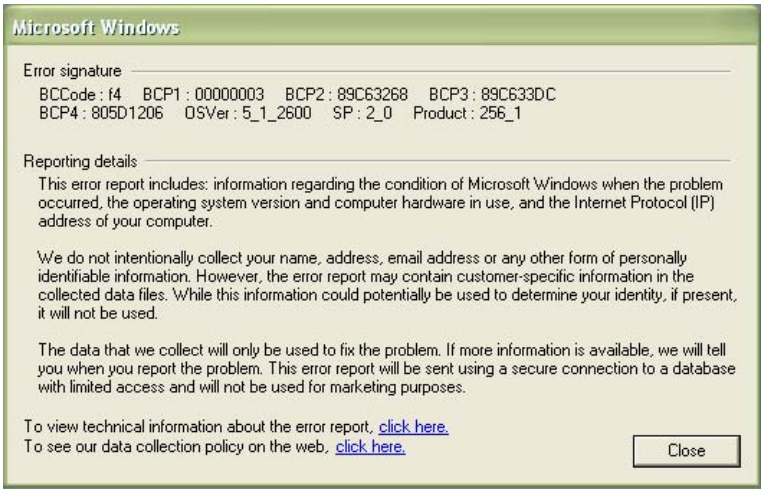

Figure 4. System error message after restarting from BSoD.

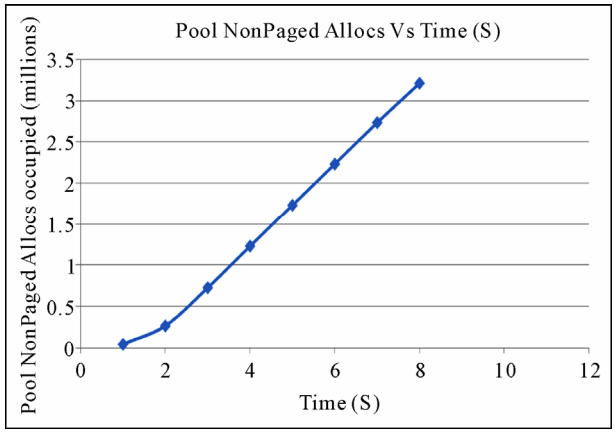

Figure 5. NonPaged pool allocs for 1 Gbps of ping traffic when McAfee firewall was in default mode.

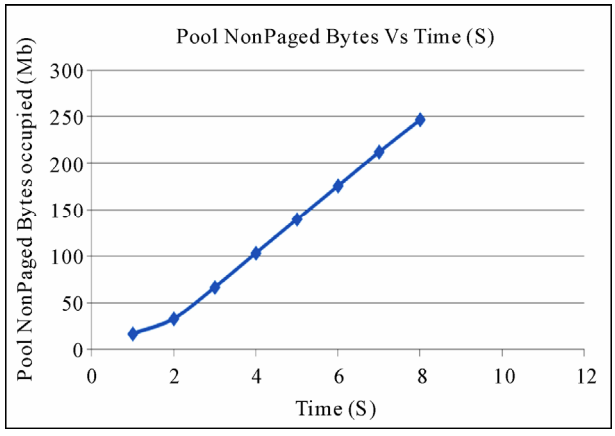

Figure 6. NonPaged pool bytes for 1 Gbps of ping traffic when McAfee firewall was in default mode.

restart we collected the "dump files" and analyzed them for the possible reasons. The main reason for this BSoD was some module named "mfehidk.sys" that was corrupting the stack, as can be known from the "Bug check Analysis". The process "mfehidk.sys" is the Host Intrusion Detection Link Driver belongs to the software McAfee, Inc [13]. From this we can know that the reason for BSoD on windows XP-SP2 with McAfee SecurityCenter was the McAfee Host Intrusion Detection Link Driver.

We tried the Ping attack one more time with the option "Allow ICMP ping requests" in **Figure 7** checked, that is we are allowing the attack now. This time the computer ran smoothly, *i.e.*, the system did not crash and the processor utilization is as shown in **Figure 8** below:

From **Figure 8** it can be seen that the average processor utilization was just 50% for 1 Gbps of traffic and the system was working properly withour freezing up. The option "Allow ICMP ping requests", as shown in **Figure 7**, tells us that the defaut mode is set to block the attack on the system, but the McAfee Firewall was unable to block it and created a Denial of Service on the host system itself by creating an exception in the memory and freezing the system resulting in the BSoD, but when we are allowing the attack, by checking the option "Allow ICMP ping requests", the system was safe with 50% of processor utilization. We observed the similar condition in other computer with Vista operating system.

The Ping attack was performed to see the performance of latest DELL Inspiron 530 desktop built on Intel Core 2 Quad 2.4 Ghz processor with Vista Business and McAfee SecurityCentre 9.3 with Personal Firewall 10.3 and 2 GB of RAM.

We consider here 2 cases

***Case* I**: McAfee Firewall was activated and was allowing incoming ICMP Echo Requests.

***Case* II**: McAfee Firewall was activated and was blocking Incoming ICMP Echo Requests.

The results in each case are detailed below:

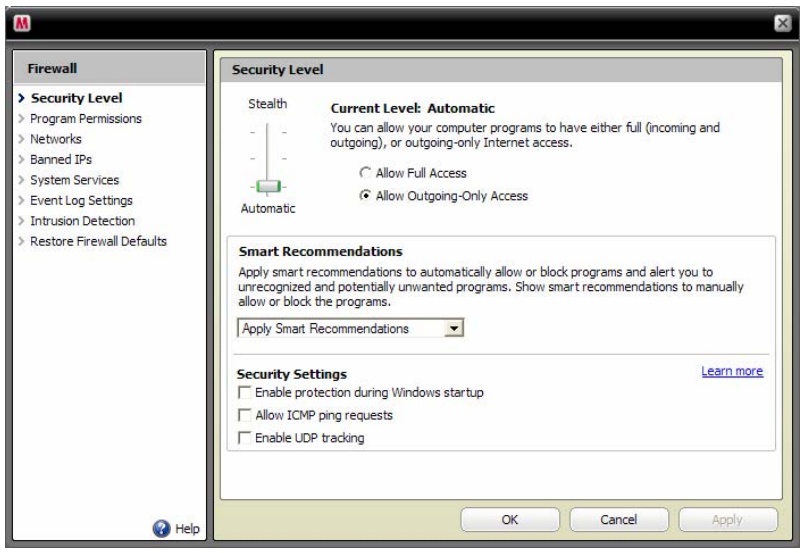

Figure 7. Default setting in McAfee firewall showing the options to allow/disallow ping and UDP traffic.

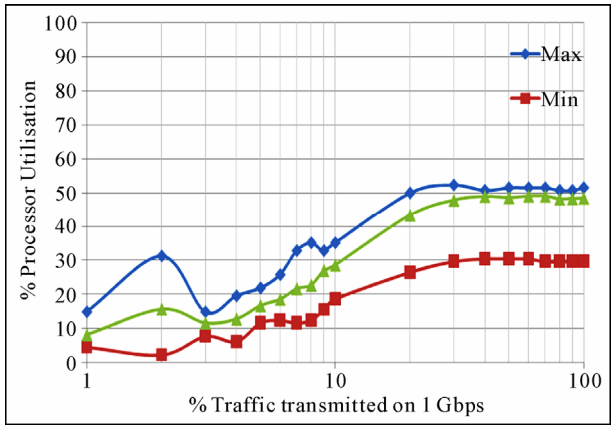

Figure 8. Processor utilization (on a logarithmic scale) of iMac deploying windows XP OS with McAfee SecurityCenter firewall under ping attack with allowing ICMP ping requests.

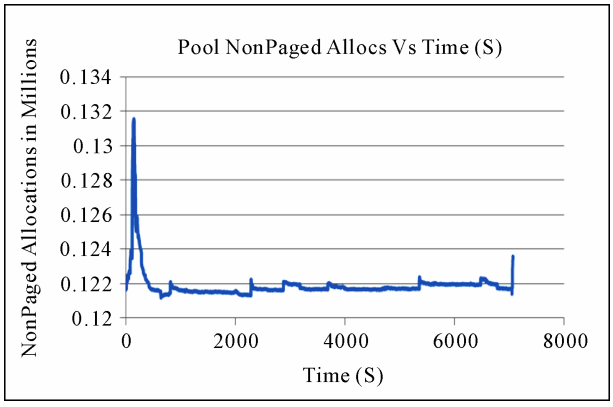

Figure 9. NonPaged pool allocation with McAfee firewall activated and allowing incoming echo request.

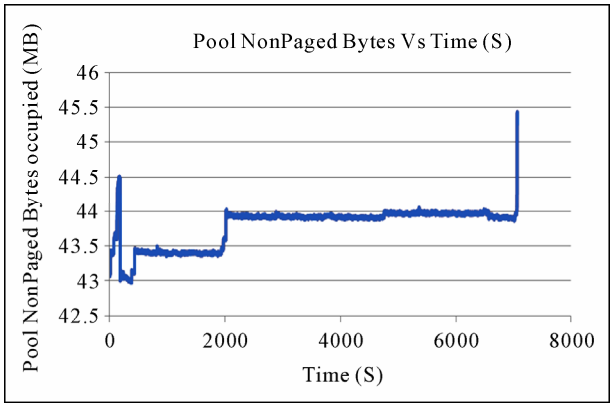

Figure 10. NonPaged pool bytes allocated with McAfee firewall activated and allowing incoming echo request.

***Case* I**:

This is the case where McAfee Firewall was activated and it was allowing Incoming ICMP Echo Request packets. Ping attack traffic is sent to the Victim computer in the range of 10% to 100% over 100 Mbps Ethernet medium.

The NonPaged Pool allocs and Bytes allocated were found as shown in **Figures 9** and **10**. The data was logged using the performance counters in windows operating system and is plotted.

***Case* II**:

This is the case where McAfee Firewall is activated while blocking the Inbound ICMP Echo request packets. Generally the results similar to case I were anticipated. But the system became non-responsive after 2.5 minutes of launching the attack with 100 Mbps of Ping attack traffic in the Fast Ethernet medium. System had to be restarted and the load of the attack traffic was reduced. To understand the system behavior the attack traffic was reduced to 1 Mbps. It was found that even with 1 Mbps

of Ping attack traffic the system froze, and was not responding after 3 hours of launching the attack.

Figures 11 and **12** show that the NonPaged pool allocs and NonPaged pool bytes occupancy in main memory due to 1Mbps of Ping traffic sent to the victim computer. It is observed that while McAfee firewall was defending the victim computer against the Ping attack; the generated NonPaged allocs consumed the entire memory resource of the victim computer which resulted in the Denial of Service attack. As no other Applications were running it was clear that McAfee itself was causing the Denial of Service attack by creating NonPaged allocs.

Figure 13 shows the Processor utilization and Memory occupancy just before the system hangs up. We can observe that the processor utilization was low and it is 34% where the entire RAM was consumed that resulted in the Denial of Service attack. This flaw that we discovered with McAfee Firewall was observed on more than one type of computer platform. We observed the same problem on XP-SP2 operating system as well as Windows Vista Ultimate 32-bit operating system. The same flaw is discovered in McAfee SecurityCentre 2010 also.

When it was installed in Vista the McAfee was consuming the entire main memory and caused the Denial of Service (DoS), whereas in XP-SP2 it was resulting in system freeze and BSoD. The reason for this is well explained in [14], where it says that: "Prior to Vista, the memory manager on 32-bit Windows calculates how much address space to assign each type at boot time. Its formulas take into account various factors, the main one being the amount of physical memory on the system. The amount it assigns to NonPaged pool starts at 128 MB on a system with 512 MB and goes up to 256 MB for a system with a little over 1 GB or more. The memory manager in 32-bit Windows Vista and later, doesn't carve up the system address statically; instead, it dynamically assigns range to different types of memory according to changing demands. However, it still sets a maximum for NonPaged pool that's based on the amount of physical memory, either slightly more than 75% of physical memory or 2 GB, whichever is smaller". This can be verified with **Figure 6** for XP where the system froze and displayed BSoD after the NonPaged bytes occupied reached nearly 250MB and **Figure 12** for Vista shows that all the available main memory, *i.e.*, nearly 1.6 GB (75% of 2 GB) out of available 2 GB of RAM is consumed.

3.3. ICMP Land Attack

This is another Layer-3 attack where the ICMP ping request packet is spoofed with destination IP host/port address same as source's. When a barrage of such Land

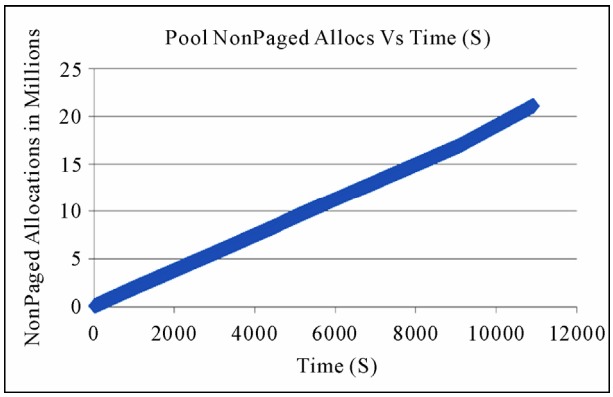

Figure 11. NonPaged pool allocs for 1 Mbps of ping traffic when McAfee firewall was activated and was configured to block ping attack traffic.

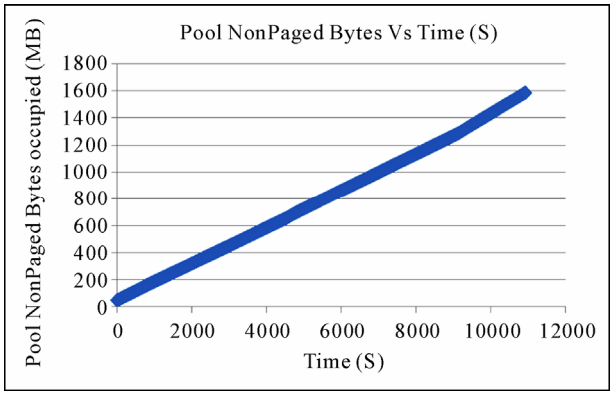

Figure 12. Pool NonPaged bytes in main memory for 1 Mbps of ping attack traffic when McAfee firewall was activated and was configured to block ping attack traffic.

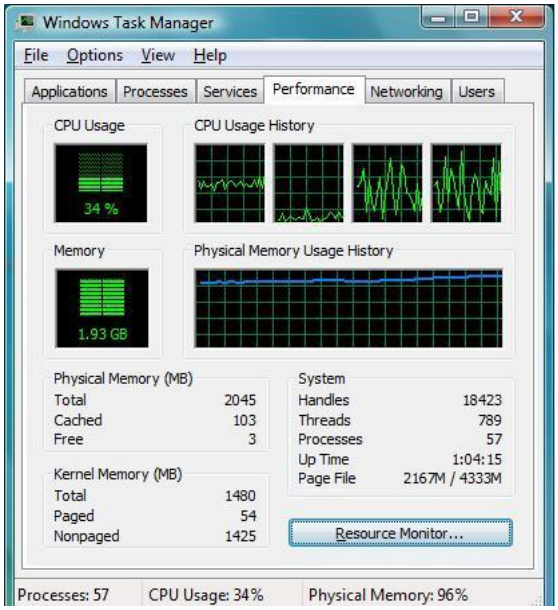

Figure 13. CPU and memory utilization just before the system hang up.

attack packets were sent the host becomes busy in replying to itself and results in system lockup. This vulnerability was found in Windows XP with SP2 service pack and also Windows Server 2003 with firewall turned off. These systems are found vulnerable for the LAND attack, which caused a temporary Denial of Service (DoS) that lasts for 15 to 30 seconds. In case of windows Server 2003 not only the server but also all workstations on the network froze [15]. A similar testing was done on Windows XP, Vista and Apple's Leopard OS, where it was found that the Windows Vista has crashed at ICMP Land attack load of 30 Mbps [16].

ICMP LAND Attack on McAfee SecurityCenter

As shown in **Figure 14** above the Average processor utilization recorded for ICMP Land attacks was nearly 70% at 1 Gbps and the attack ran smoothly and the system was working normally without giving any of the effects described in case of ping attack.

3.4. TCP-SYN Flood Attack

TCP flood attack is Layer-3 attacks, which is most popular denial of Service attack that exhausts the system resources and brings many serious threats to the entire network. The host retains many half open connections and there by exhausts its memory and processor utilization. The Transmission Control Protocol (TCP) that is built on IP has a three-way handshake process for any connection establishment. When a client initiates the TCP connection, it send a SYN packet to the server and then the server responds with an SYN-ACK packet and stores the request information in memory stack. After receiving the SYN-ACK packet the client should confirm the request by sending an ACK packet. When the server receives the ACK packet it checks in the memory stack to see whether this packet corresponds to previously received SYN. If it is, then the connection is established between the client and the server and data transfer can be started. This is the Three-way handshake method used to establish a connection using TCP protocol. In TCP-SYN Flood attack, the attacker sends a barrage of SYN packets with spoofed IP address to the server and the server stores that information in the memory stack, sends the SYN-ACK and waits for the final ACK from the attacker. But the attacker will not send the ACK so such connections will be left in the memory stack. This process consumes considerable memory as well as processor utilization of the server. If large amounts of SYN attack packets were sent then a Denial of Service attack can be launched on the victim. There are many methods suggested to fight against this TCP-SYN attack [17-19]. Service packs and some firewalls have also been evaluated to measure their effectiveness in mitigating the DoS [20-22] attacks.

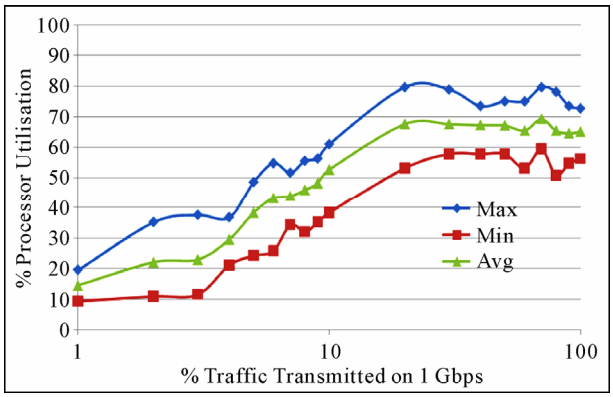

Figure 14. Processor utilization (on a logarithmic scale) of the iMac computer deploying XP-SP2 OS, with McAfee Firewall at default settings due to ICMP Land attack.

TCP-SYN Attack on McAfee SecurityCenter

TCP-SYN flood is Layer-4 Denial of Service attack. TCP-SYN attack traffic is sent to the iMac deploying WindowsXP-SP2 with McAfee Firewall at default settings and there is no option to avoid the TCP-SYN attack. After we started the TCP-SYN attack, the system froze giving us the BSoD again, as in the case of Ping attack. The processor utilization was just 50% for 1 Gbps of traffic and the Pool NonPaged Allocs and Bytes were plotted as shown in the **Figures 15** and **16**. These are very much similar to the case where Ping attack was done and the reason was the same. McAfee Firewall is creating NonPaged allocations that are growing unboundedly in the main memory and cannot be paged out. The operating system cannot allocate more than the assigned memory so it is causing in system freeze and resulting in BSoD. It can be observed that it took 8 seconds for the system to freeze from the **Figures 15** and **16**.

3.5. UDP Flood Attack

DDoS attack using the UDP packets is called UDP Flood attack. UDP Flood attack is a Layer-4 attack. Specialists have discovered the UDP Flood vulnerabilities during the year 1998-2000 in many systems including Microsoft products. In UDP Flood attack a barrage of UDP packets are sent to the victim computer either on specified ports or on random ports. The victim computer processes the incoming data to determine which application it has requested on that port and in case of absence of requested application on that port, the victim sends a "ICMP Destination Unreachable "message to the sender, which is generally a spoofed IP. If such a barrage of requests were sent then it results in Denial of Service on the victim

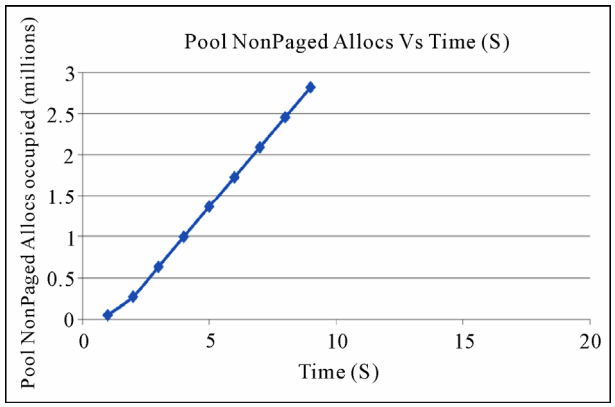

Figure 15. NonPaged Pool Allocs for 1 Gbps of TCP-SYN Flood when McAfee Firewall was in default mode.

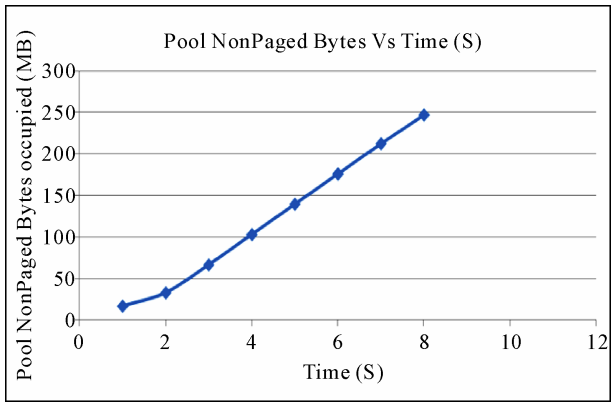

Figure 16. NonPaged Pool Bytes occupied for 1 Gbps of TCP-SYN Flood when McAfee Firewall was in default mode.

computer as the victim will become busy in processing those packets and sending ICMP Destination Unreachable messages. UDP flood attacks may also depletes the bandwidth of network around the victim's system. For example, by sending UDP packets with spoofed return addresses, a hacker links one system's UDP character-generating (chargen) service to another system's UDP echo service. As the chargen service keeps generating and sending characters to the other system, whose echo service keeps responding, UDP traffic bounces back and forth, preventing the systems from providing services [21].

UDP Flood Attack on McAfee SecurityCenter

The system froze in this case also giving us the same BSoD and the "dump crash files" are analyzed and found out to be the same reason as in case of Ping and TCP-SYN attacks. McAfee is causing unbounded growth of NonPaged pool allocation that's filling up the memory and hence resulting in system BSoD.

In case of UDP Flood attack even with the option "Allow UDP Tracking", as shown in **Figure 7**, checked the system still freezes and results in BSoD.

4. Conclusions

Our experiments with real attack traffic show that McAfee firewall is able to defend against some attack traffic but not others. We can observe that McAfee is able to defend ARP-based flood and ICMP Land Attacks but was not able to defend other attacks and became the reason of Denial of service by itself on the host, which it has to protect. The possible reasons for the unbounded growth of Nonpaged pool Allocations were:

- Unexpected driver code path.
- Intermediate returns from functions that allocated the NonPaged pool memory (memory leaks).
- Bug fixes or work arounds, that added a new piece of code to allocate, but forgot to disallocate.
- Unexpected sequence of hardware Events/Behavior that called the buggy ISRs (Interrupt Service Routine).
- Mis-communication between modules of driver and or OS components.

ARP-based flooding attack usually happens in the LAN as it is a Layer-2 attack. McAfee SecurityCentre is allowing ARP attack as it mainly concentrates on internet based flooding attacks. In case of PING, TCP-SYN and UDP Flood attacks, the attack packets are coming from different IP addresses that are usually spoofed and McAfee may be allocating more Nonpaged memory for defending these types of attacks per each packet it receives and as there will be lot of hosts attacking, it's creating a lot of NonPaged allocs and trying to occupy the RAM, thereby creating BSoD in XP and system get freeze due to RAM unavailability in Vista. This is because in the ICMP land, the attack packets are crafted as if they are originating from one IP address, that is usually its own IP, so it's not creating more processes and hence is not creating any Denial of Service by itself on the host.

5. Acknowledgements

This work was supported in part by the funding from U.S. National Science Foundation, Grant No: 0521585.

6. References

[1] McAfee Claim, 2009. http://us.mcafee.com/root/landingpages/affLandPage.asp?affid=0&lpname=14229&cid=41183

[2] Latest DDoS Attack on Twitter, 2010. http://status.twitter.com/post/157191978/ongoing-denial-of-service-attack

[3] Latest DDoS Attack on Twitter and Facebook, 2010. http://www.techcrunch.com/2009/08/06/ddos-attacks-cru

sh-twitter-hobble-facebook

[4] US, South Korean Websites under Attack, 2010. http://government.zdnet.com/?p=5093

[5] US Government Sites Bombarded by Botnet, 2010. http://news.techworld.com/security/118814/us-government-sites-bombarded-by-botnet/

[6] S. Kumar, M. Azad, O. Gomez and R. Valdez, "Can Microsoft's Service Pack 2 (SP2) Security Software Prevent Smurf Attacks?" *Proceedings of the Advanced International Conference on Telecommunications* (*AICT*'06), Le Gosier, 19-22 February 2006.

[7] S. Gaudin, "DoS Attack Cripples Internet Root Servers," 2010. http://www.informationweek.com/news/internet/showArticle.jhtml?articleID=197003903

[8] NonPaged Allocations in Microsoft Windows, 2010. http://technet.microsoft.com/en-us/library/cc778082(WS.10).aspx

[9] Information on Pool Resources, 2010. http://blogs.technet.com/askperf/archive/2007/03/07/memory-management-understanding-pool-resources.aspx

[10] D. C. Plummer, "Ethernet Address Resolution Protocol," IETF Network Working Group, RFC-826, 2010. http://www.ietf.org/rfc/rfc826.txt

[11] J. Postel, "Internet Control Message Protocol," IETF Network Working Group, RFC-792, 2010. http://tools.ietf.org/html/rfc0792

[12] S. Kumar, "PING Attack—How Bad Is It?" *Computers & Security Journal*, Vol. 25, No. 5, July 2006, pp. 332-337.

[13] Information about Mfehidk.Sys File, 2010. http://www.file.net/process/mfehidk.sys.html

[14] NonPaged Pool Allocation in Windows, 2010. http://blogs.technet.com/markrussinovich/archive/2009/03/26/3211216.aspx

[15] Possible LAND Attack Vulnerability Affects Windows XP and 2003, 2010. HTTP://articles.techrepublic.com.com/5100-10878_11-5611467.html

[16] S. Raj, V. Hari and S. Kumar, "Performance of Windows XP, Windows Vista and Apple's Leopard Computers under a Denial of Service Attack," 2010 4*th International Conference on Digital Society*, (*ICDS* 2010), St. Maarten, 10-16 February 2010.

[17] P.-E. Liu and Z.-H. Sheng, "Defending against TCP-SYN Flooding with a New Kind of SYN-Agent," *International Conference on Machine Learning and Cybernetics*, Vol. 2, 12-15 July 2008, pp. 1218-1221.

[18] Shakhov, V. Vladimir and H. Choo, "On Modeling Counteraction against TCP SYN Flooding," 21*st International Conference on Information Networking*, *ICOIN* 2007, Estoril, 23-25 January 2007.

[19] W. Chen, D.-Y. Yeung and P.-E. Liu, "Defending Against TCP SYN Flooding Attacks under Different Types of IP Spoofing," *International Conference on Networking Systems and International Conference on Mobile Communications and Learning Technologies*, *ICN*/*ICONS*/*MCL* 2006, Morne, 23-29 April 2006, p. 38.

[20] S. Kumar and E. Petana, "Mitigation of TCP-SYN Attacks with Microsoft's Windows XP Service Pack2 (SP2) Software," 7*th International Conference on Networking*, *IEEE*, Cancun, 13-18 April 2008.

[21] F. Lau, S. H. Rubin, M. H. Smith and L. Trajkovic, "Distributed Denial of Service Attacks," *IEEE International Conference on Systems*, *Man*, *and Cybernetics*, Nashville, 8-11 October 2000, pp. 2275-2280.

[22] S. Surisetty and S. Kumar, "Is McAfee SecurityCenter/Firewall Software Providing Complete Security for your Computer?" 4*th International Conference on Digital Society*, (*ICDS* 2010), St. Maarten, 10-16 February 2010.

