Global Information Assurance Certification Paper

Denial of Service Attacks and Windows XP:

Separating Fact from Fiction

Feeroz Rani Mirza
Version 1.2e

Denial of Service Attacks and Windows XP: Separating Fact from Fictions

The recent uproar in regards to Windows XP has rejuvenated the spotlight on Distributed Denial of Service Attacks (DDoS)/Denial of Service Attacks (DoS), and how anyone and everyone is vulnerable to this extremely damaging attack. DDoS/DoS will be used interchangeably in the research paper. Gibson Research Corporations (GRC) recently posted a statement on its web site claiming that the inclusion of a "raw sockets" implementation in Microsoft Windows XP will aid Internet vandals in carrying out a distributed denial of service attacks[1]. On the contrary, Microsoft feels the presence of operating system-level functions to manipulate data packets is not a critical factor in the number of DDoS attacks. In fact, if this were true, the explosion in DDoS attacks should have already occurred seeing as raw sockets are implementations are already present in Linux, VMS, Mac OS X, and even previous versions of Windows.[2] The real issue is whether the attacker could run hostile code on another user's computer. Like viruses, Trojan horses and other hostile code, a zombie program can only run if an attacker can install it and run it. [2] A zombie is a program that sends out so many data packets as such a rate that the system is overloaded and unable to respond to requests from legitimate users. The fact remains. DDoS/DoS attacks have been extremely successful in having systems and networks become inoperable. There are precautionary measures one can follow take to mitigate the risk to the network or system against a DDoS attack, however current technology to thoroughly defend against this sort of attack is greatly lacking, or sorry to say, non-existent.

Background on DDoS/DoS attacks:

DDoS attacks are aimed at devices and networks expose to the Internet. Their goal is to cripple a device or network so that external users no longer have access to your network.[4] The following are a few examples of DDoS/DoS attacks:

Smurf Attack: A brute force attack that floods your routers with Internet Control Message Protocol (ICMP) echo request packets. ICMP is used for error messages, such as "host unreachable" and ICMP messages are interpreted by the network software. Getting back to the Smurf Attack, the destination IP address of each packet is the broadcast address of your network. The router will then broadcast the ICMP echo request packet to all hosts on the network. If numerous hosts are involved, this will create large amounts of ICMP echo request and response traffic. Additionally, if the source IP address of the ICMP echo request packet is spoofed, this traffic will clog up the network and also congest the network of the spoofed source IP address. IP spoofing is making a distinct computer believe that the information sent to it is from a trusted system, when in fact it is not. More than likely the main goal of an attacker will be to gain root access to the

[1] Gibson, Gibson Research Corporation, http://grc.com/dos/grcdos.htm.
[2] http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/raw_sockets.asp

[4] Downey, http://www.zdnet.com/pcmag/pctech/content/17/08/nt1708.001.html

host, and create a backdoor into the target system.

Ping of Death: Uses a ping system utility to create an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system. The system may crash, hang, or reboot when such a maliciously crafted packet is received.

Teardrop Attack: Exploits weaknesses in the reassembly of IP packet fragments. The Teardrop program creates a series of IP fragments with overlapping offset fields. Once these fragments are reassembled at the destination host, the system may crash, hang, or reboot.

Windows XP:

Windows XP (code-named "Whistler" in beta form) is Microsoft's long-awaited operating system that builds on the strengths of Microsoft Windows 2000, while incorporating and expanding the consumer-friendly potential of Windows Millennium Edition (Me). [5] Windows XP is based on the Windows 2000 code base and inherits both Windows 2000 and Windows Me reliability and performance. For client machines, Windows XP has two editions, Professional and Home. On the server side, the three editions match the current Windows 2000 server configurations: Server; Advanced Server for departmental servers, line-of-business, and Web-enabled applications; and Datacenter Server, for high-availability, mission-critical applications. The server editions have their own similar feature set. [4]

Windows XP includes several new features, for example, new visuals, high-quality icons, many task bar improvements. Windows XP desktop themes change the way controls, windows boarders, and menus are drawn. The applications in Windows XP adopt a side-by-side versioning strategy. For background on side-by-side component sharing issues and DLL redirection, see Implementing Side-by-Side Component Sharing in Applications (Expanded) by David D'Souza, BJ Whalen, and Peter Wilson.[4] Windows XP also brings a new feature called fast user switching, which is based on the computer sharing functionality of Windows 2000 and Windows 2000 Terminal Server. This additional feature allows several users to effortlessly and efficiently share the same computer.

The Windows XP operating system is due out in the second half of 2001. Microsoft claims, “Windows XP will be the highest quality Microsoft operating system ever”. [8] The

---

[5] Marsh, Massy, and Boylan, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwxp/html/winxpintro.asp

[8] Rubley, http://www.zdnet.com/pcmag/stories/trends/0,7607,2717512,00.ht

product is said to be more stable and fault tolerant the previous versions, with many new interface enhancements. On the security side, Microsoft claims that Windows XP is less vulnerable to hackers who want to plant Trojan horses on Windows PC. [9] It is strongly felt by Microsoft, that the real issue is whether the attacker could run hostile code on another user's computer, ie. viruses, trojan horses and other hostile code, a zombie program can only run if an attacker can install it and run it. However, raw socket implementation, to be discussed in further detail later in this paper, will allow a computer running Windows XP to generate a "spoof" IP address, meaning there is no way for the target of a DDoS attack to identify the genuine IP address of the machines attacking it. [10] With this feature, there will be no true way for a web site to defend itself against such a flood of packets. You will not be able to distinguish incoming hacker traffic from the ordinary customer traffic. Windows 9x PCs are able to send IP packets using valid IP addresses, which makes filtering out bad packets an option in an DDoS attack, unlike with Windows XP where IP spoofing with be a serious issue.

There is another feature of Windows XP worth mentioning which has security ramifications but beyond the scope of this paper – Smart Tags. Smart Tags allows Microsoft's Internet Explorer browser, which is included in Windows XP, to turn any word on any web page into a link to a website approved by Microsoft. This feature enables Microsoft, through the browser running on your system, to modify any website, without the owners knowledge or permission. This feature tempts and encourages users to leave and go to sites chosen by Microsoft.

Brief Definition of TCP/IP:

Transmission Control Protocol/Internet Protocol (TCP/IP) is a protocol suite that allows computers of all sizes, from several different computer vendors, running entirely dissimilar operating systems, to communicate with each other. A protocol suite such as TCP/IP is a combination of different protocols at various layers, and normally considered to be a four-layer system, as shown in figure 1.1. [11]

Application	Telnet, FTP, e-mail, etc.
Transport	TCP, UDP
Network	IP, ICMP, IGMP
Link	Device driver and interface card

Figure 1.1 The four layers of the TCP/IP protocol suite.

WindowsXP: A threat in assisting future DDOS attacks?

---

ml

[9] http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/raw_sockets.a
sp

[10] Wearden, http://www.zdnet.com/zdnn/stories/news/0,4586,2770517,00.html?&_ref=178282959
4.

[11] Stevens, page 2

GRC's claims there are a set of functions, know as "raw sockets" included in the Windows XP networking services that will enable programs to manipulate the construction and content of Transmission Control Protocol Internet Protocol (TCP/IP) data packets. Raw sockets enable a machine to send or capture data independent of the operating system. [12] This feature in Windows XP's architecture opens up a frightening security hole which could make it easier for malicious programmers to launch a DDoS attacks which brought down many large e-commerce sites in the past. [13] Windows XP will entail the ability for any application to send packets bearing faked or spoofed IP addresses. GRC's perception that this functionality will increase the incidence of DDoS attacks, in which a malicious user clandestinely installs "zombie" software on other people's computers and then directs the zombies to combine forces and floods the target network with data. A zombie program running on Windows XP could use native operating system function to disguise the originating point of data, know as IP spoofing. IP spoofing is fooling a distant computer into believing they are a legitimate member of the network in order to gain access to the network.

In the current version on Windows, Winsock overwrites a packet's source IP address with the systems true IP address before sending the packet to its destination. Winsock is an open network Application Programming Interface (API) standard. It was first designed to create a standard programming interface for TCP/IP on all versions of Microsoft Windows including Windows 2000, Windows NT, Windows 95/98, Windows CE and Windows 3.x. [14] Some of the major benefits of Winsock are that it provides an open API standard rather than a closed proprietary API, and it has helped further the success of TCP/IP with the Microsoft Windows operating systems. Secondly, application developers have been able to easily port applications from BSD (Berkley Standards Distribution) Sockets source code to run on all Windows platforms. Finally, Winsock has made it much easier for end users and information technology managers to find a wide selection of the applications to choose from that can run "out of the box." without modification. [11]

In addition, it may be true that raw sockets are available in Windows 2000 and Unix, however, Unix servers usually have trained administrators, many of whom have taken steps to prevent recurrences of security breaches. Most home users do not have any formal security training. Windows XP has taken steps to try to make the operating systems less vulnerable by adding a "Personal Firewall" and "Software Restriction Policy", this feature specifically "may" be off by default, but is currently "an area being looked at" by Microsoft".[16]

Steve Gibson of GRC states, "It is impossible for an application running under any version of Windows 3.x/95/98/ME or NT to "spoof" its source IP or generate malicious TCP packets such as

---

.

[12] Greene, http://www.theregister.co.uk/content/6/19623.html?&_ref=9748013
7)

[13] Knight, http://news.zdnet.co.uk/story/0,,s2076896,00.htm
l

[14] http://www.stardust.com/winsock/intro.h
tm

[16] Livingston, InfoWorld, page

SYN or ACK floods. [17] In addition, Steve feels that when those insecure and maliciously potent Windows XP machines are mated to high-bandwidth Internet connections, we are going to experience an escalation of Internet terrorism the likes of which has never been seen before. [13]

Microsoft's Claim/Defense

Microsoft states that raw sockets and the ability to spoof IP addresses add little to the problem of DDoS/DoS attacks, saying that hostile code is the real problem. [18] An intruder can install hostile code (e.g., DDoS Trojans) on a user's machine, and at the same time nothing prevents the intruder from installing a custom packet driver, capable of spoofing IP addresses at the same time. It further pointed out that other operating systems, VMS, Mac OS X, Linux, various version of Unix, have allowed IP address spoofing for a long while. In addition, Microsoft states that if an explosion of DDoS attacks were going to occur, it would have already happened on other operating systems. [19]

The threat of DDOS already exists, how to currently defend again DDOS/DOS attacks, the REAL threat:

One of the more common methods of defending your system or network against a "denial of service" attack is to set up a filter, or "sniffer," on a network before a stream of information reaches a site's Web servers. A filter is software that can look for attacks by noticing patterns or identifiers contained in the information. If a pattern comes in and is noticed frequently, the filter can be instructed to block messages containing that pattern. This will protect the Web servers from having their lines tied up.

When used in conjunction with new tools such as Zombie Zapper, and a solid set of security practices can do the most to protect computers from becoming unwitting accomplices in DoS attacks. Zombie Zapper is a free, open source tool that can tell a zombie system flooding packets to stop flooding. [20]

Many thoughtful and well-informed people have suggested that the real responsibility for stopping these attacks lies not with the behavior of the user and/or their Internet-connected machine (e.g. Windows XP), but with the Internet's ISP's. [21] In utilizing "network egress filtering", the Internet Service Provider becomes responsible for curtailing the IP spoofing of their own users. Egress or Outbound filtering blocks traffic with an invalid source IP address. This keeps a denial of service attack using IP address spoofing from originating on the internal network. The filter should only allow traffic to leave your network with a source IP address that is

---

60.

[17] Gibson, http://grc.com/dos/grcdos.
htm

[18] http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/raw_sockets.
asp

[19] http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/raw_sockets.
asp

[20] http://razor.bindview.com/tools/ZombieZapper_form.sht
ml

[21] Gibson, Gibson Research Corporation, http://grc.com/dos/winxp.

valid on your internal networks. The purpose here is to keep a denial of service attack from originating on the private network. [22]

Several leading sites were hacked and fell victim to a DDoS attack. DDoS attack tools are more of a threat to individuals who have full-time connection to the Internet. The most disturbing fact remains that, many of the same sites that have fell victim to a DDoS remain virtually powerless to stop such attacks. Despite vendors' efforts in the wake of last year's incidents to prevent future attacks, security experts say there's still no solution available that can fully protect a site from DDoS attack, a fact not lost on the sites hit last year. [23] The real backbone of any network security system should be constant monitoring. [19]

Another way of protecting your system or network against a DDOS is to adopt the concept of "Defense in Depth". [25] Simply put, if one level of security fails, there is another layer or backup to defend the system or network. The key areas of Defense in Depth are as follows: [20]

- Perimeter Security (ie. Firewall)
- Anti-Virus Software
- Basic Auditing (NT/UNIX/LINUX)
- What is your role and responsibilities for these?

Conclusion:

The development of Windows XP only assists in facilitating hackers, script kiddies, with another way to become a nuisance, and more than likely damaging. Along with this, as DDoS attacks continues to evolve as new more damaging and potent methods are continually developed, the threat will become more severe. Several people I have spoken with in regards to Windows XP and DDoS attacks, make the comparison to DDoS attacks with car jacking. The feeling is, if car thieves want a car bad enough, they will find a way to get the car. Again, for example, I equate the "script kiddies" to "joy riding", there are basic security safeguards that may be put in place to mitigate some risk, ie. Defense in Depth. These procedures can be followed to possibly lessen the possibility of a DDoS attack, as well as car theft by less experienced car thief. On the same note, encouraging damaging acts are not the way to go. I feel with the development of Windows XP, there will be a great increase in future DDoS attacks with Windows XP directly involved in many of those attacks.

---

htm

[22] Strom, http://www.sans.org/infosecFAQ/firewall/packet_filter.
htm

[23] Lemos, http://www.zdnet.com/filters/printerfriendly/0,6061,5092020-2,00.ht
ml

[25] Harris, Cole, SANS Level Once:Security Essentials, page 1

List of References:

Boylan, John March, Kyle Massy, Dave. "Microsoft Windows XP: What's in It for the Developers?". Februray, 2001. **http://www.zdnet.com/pcmag/pctech/content/17/08/nt1708.001.html** June 4, 2001.

Cole, Eric Harris, Daniel. LevelOne SANS Security Essentials, Part 1. Baltimore:SANS Institute, May 2001. Page 1-21.

Downey, Jeff. "Denial-of-Service Attacks". April 28, 1998. **http://www.zdnet.com/pcmag/pctech/content/17/08/nt1708.001.html** June 1, 2001.

Gibson, Steve. "Why Windows XP will be DENIAL OF SERVICE Exploitation Tool of Choice for Internet Hackers Everywhere". June 2, 2001. **http://grc.com/dos/winxp.htm** June 11, 2001.

Gibson, Steve. "The Strange Tale of the DENIAL OF SERVICE Attacks Against GRC.COM". June 2, 2001. **http://grc.com/dos/grcdos.htm** June 11, 2001.

Greene, Thomas. "Security geek developing WinXP raw socket exploit". June 6, 2001. **http://www.theregister.co.uk/content/6/19623.html?&_ref=1556661854** June 11, 2001.

Knight, Will. "Special: Denial of Service round-up". February 9, 2001. **http://news.zdnet.co.uk/story/0,,s2076896,00.html** May 3, 2001.

Lemos, Robert. "DoS attacks: No remedy in sight". June 1, 2001. **http://www.zdnet.com/filters/printerfriendly/0,6061,5092020-2,00.html** June 5, 2001.

Livingston, Brian. "Windows XP and DDos". InfoWorld. Issue 24 June 11, 2001. Page 60.

Rupley, Sebastian. "Now Due In October: Windows XP". May 10, 2001. **http://www.zdnet.com/pcmag/pctech/content/17/08/nt1708.001.html** May 5, 2001.

Stevens, Richard. TCP/IP Illustrated , Volume 1. Reading: Addison Wesley Longman, 1994.

Strom, Dan. "The Packet Filter: A Basic Network Security Tool". September 25, 2001. **http://www.sans.org/infosecFAQ/firewall/packet_filter.htm** May 20, 2001.

Wearden, Graeme. "Battle rages over Windows XP security". June 7, 2001. **http://www.zdnet.com/filters/printerfriendly/0,6061,2770517-2,00.html** June 4, 2001.

"Hostile Code, not the Windows XP Socket Implementation, is the Real Security Threat". **http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/raw_sockets.asp** June 15, 2001.

"Introduction: What is WinSock?". **http://www.stardust.com/winsock/intro.htm** June 11, 2001

"Zombie Zapper Download". **http://razor.bindview.com/tools/ZombieZapper_form.shtml** June 10, 2001

Last Updated: July 28th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event