Windows XP and full raw sockets: A new security concern from home-based PC's or a desirable new function?

Jim Kehres
GIAC Security Essentials
Version 1.2e
08/10/2001

Windows XP and full raw sockets: A new security concern from home-based PC's or a desirable new function?

You login to your computer and try to access the following sites: www.yahoo.com, www.microsoft.com, www.ebay.com, etc... After a few seconds your web browser displays something similar to the following:

This page cannot be displayed
The page you are looking for is currently unavailable

Cannot find server or DNS error

While you may think something is wrong with your computer or your Internet connection, you have actually just witnessed the effects of a Denial of Service attack (DOS). A Denial of Service attack makes a particular destination on the Internet inaccessible by inundating it with bogus traffic. Currently, these attacks are estimated to occur at a rate of more than 4,000 per week, according to a recent study by the University of California at San Diego.(Ploskina) While that number may seem rather exorbitant, researchers say it is a conservative estimate and others feel the worst is yet to come.

A new potential threat that could exacerbate this problem may come with the release of Windows XP. This new version of Windows will be aimed at corporate AND consumer markets. The potential threat involves the inclusion of fully supported raw sockets with Windows XP and the reality that it will eventually be installed on millions of unsophisticated home-user's computers in the near future. Some feel that this will make it much easier for a hacker to spoof an IP address and perform Denial of Service attacks that will be more difficult to trace. Others feel that the availability of full raw sockets will make it possible to create more powerful features in the new version of Windows. They also believe in the fact that if malicious software is not able to infect a system, then using raw sockets to produce a negative impact on the Internet such as a DOS, will not be possible no matter the operating system's (OS) default capabilities. To begin with we will look at what raw sockets are and how it can be used for malicious intent.

The Threat of Full Raw Sockets Support

So what are raw sockets and what are the drawbacks in having an operating system fully support them? In order to even attempt to answer this question we must first go over the fundamentals of raw sockets to better understand their purpose. Steve Gibson's site (grc.com/dos/winxp.htm) covers it well as he explains how it began back in 1981 with the Computer Systems Research Group (CSRG), at the University of California at Berkeley. They created a "TCP/IP Stack" and "Berkeley Sockets" for Unix to aid in the task of creating Internet-communicating applications. One of these sockets is called the standard socket as shown in Figure 1 below. The standard socket is used to transfer data via TCP or UDP between machines. In addition to transferring data between machines, other “non-data” information must also be transmitted between machines to ensure efficient use of the Internet. To perform this function, they created the ICMP (Internet Control Message Protocol). While the operating system’s built-in TCP/IP stack handles most of this “non-data” ICMP traffic, the Berkeley designers knew it would be beneficial if programmers could generate this traffic themselves when creating applications. As shown in Figure 1 below, this is done through the use of the raw socket, which basically “short-circuits the TCP/IP stack to open a backdoor directly into the underlying network data transport. This provides full and direct packet level Internet access to any Unix sockets programmer.” (Gibson)

Figure 1 – http://grc.com/dos/winxp.htm

So what does this have to do with Windows XP? For starters, Windows XP as well as its predecessor Windows 2000 both allow full access to raw sockets. Winsock, as it is called when referring to Windows Operating Systems, did not always allow full access to raw sockets.

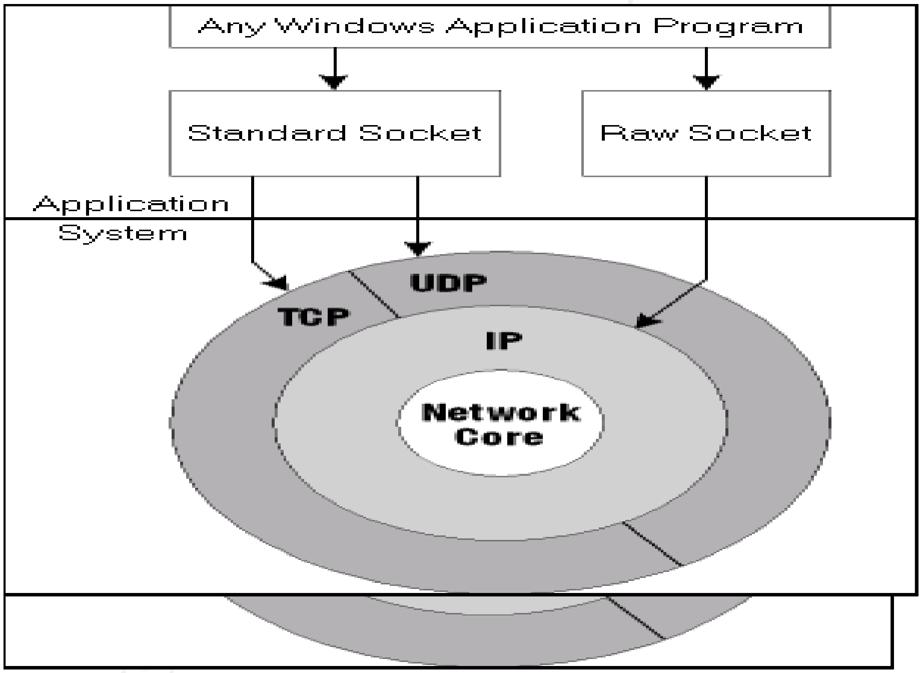

Figure 2 - http://grc.com/dos/winxp.htm

In Figure 2 above, we see that versions prior to Windows 2000 do not penetrate the encompassing IP wrapper layer.

Since versions prior to Windows 2000 did not, by default, allow access to the underlying network data transport, things like IP spoofing (which means changing the IP address of where packets originated from), were much more difficult to perform. Notice I said, “more difficult” and NOT impossible. The reason it is not impossible is due to the fact that device drivers can be created to effectively spoof an IP address on pre-Windows 2000 operating systems. The difficulty is in the fact that this additional code must infiltrate and execute on the compromised machine. This adds an extra layer of complexity that the malicious hacker must deal with since access to full raw sockets is not available by default in these older operating systems.

The argument against a machine having easy access to the raw sockets to more easily spoof an IP address is that it can be used in a Denial of Service attack that would make it more difficult to eradicate. While Windows 2000 does in fact already include this capability in Winsocks, this version of Windows is used mainly by corporate environments. Corporate environments, for the most part, protect their systems much more than consumers. The real concern is that Windows XP will be marketed to the consumer industry as well. Since consumers do not typically understand or have the knowledge to fully protect their systems, the potential for hackers to easily exploit this vulnerability is more compelling. Yes, the malicious hackers must still infiltrate the computer and execute software to perform their duties, but now it will, in essence, take less to do more harm. Once inside the computer, a hacker could more easily code a program (Trojan) to perform a Denial of Service attack with a spoofed IP address and it will be more difficult to stop since you will not know where the attack is coming from. If the malicious hacker is able to do this on a number of machines connected via a broadband connection, they can execute a very effective and powerful Distributed Denial of Service attack. These attacks involve many machines, hence the word Distributed, so the attacks are more potent. If you are able to stop one of the IP addresses or computers from attacking, the other compromised machines will still attack. Shutting these down would take more effort, which translates into time, which translates into money!

Another interesting fact is that the most complex, potent and untraceable Distributed Denial of Service and Denial of Service attacks have only come from Unix based operating systems. (Gibson) The fact that Unix based systems have full support to raw sockets are the only reason these attacks are possible. Soon this same capability will be available on thousands if not millions of home user's computers.

Stop Crying Wolf!

If you are thinking that the above fear regarding full access to the raw socket is a "bunch of malarkey", you are not alone. Obviously the main challenger to the theory above, brought about by Steve Gibson of grc.com, is Microsoft. Microsoft has even issued a press release that says, "In sum, it doesn't matter what networking functions are available as part of an operating system if an attacker's code never gets the opportunity to run on it. Microsoft is taking steps to ensure that Windows XP is the most secure operating system we have ever delivered." (Microsoft) What they mean by this is that the concern should not lie in how easy it is to get the operating system to perform undesirable tasks, at least according to the Internet, but rather we should ensure that only authorized programs are allowed to execute on any operating system. It is also a fact that other operating systems, particularly that of the Unix family, have always had the ability to spoof an IP address quite easily; yet, Denial Of Service attacks have not become the "end of the Internet". While it is true that other operating systems do allow these functions, it is also true that millions of them are not in the hands of inexperienced home users so we wouldn't have as large of an impact. In it's efforts to prevent hostile code from even getting on the system in the first place, Microsoft has implemented the following preventive measures:

- Internet Connection Firewall in Windows XP, which effectively makes Windows XP users invisible on the Internet.

- The Outlook Email Security Update, which is included in Outlook 2000 Service Pack 2 and Office XP, and prevents email attachments from being launched.
- Software Restriction Policies in Windows XP, which allow a Windows XP system to be configured so that specific classes of code and script cannot run.
- Outlook Express 6 in Windows XP which, like Outlook 2000 Service Pack 2 and Office XP, will include changes that make it significantly more difficult for an attacker to run code via HTML e-mail.

(Microsoft)

While this may assist in preventing malicious code from getting onto Windows XP, we know that it will only be a matter of time before vulnerabilities are discovered and hackers will find ways into Windows XP.

So what is Microsoft to do? Well, besides disabling full access to raw sockets in its upcoming version of Windows, a feature which Steve Gibson from grc.com claims is not needed in a consumer OS, they could invoke the help of the Internet Service Providers (ISP). The way the ISPs can assist in minimizing the threat of Denial of Service attacks is by implementing a router function called Egress filtering.

Egress filtering is a filter enabled on the ISPs router which only allows authorized IP addresses out to the Internet. Why is this important? Because if an ISP allows only an authorized range of IP addresses to leave it's control, then someone trying to spoof IP addresses on their machines would not accomplish anything if it did not fall into that range. One way around this is to spoof within the range of the hundreds or thousands of IP addresses that the ISP has under it's control, but at least it adds one more layer of complexity which may deter most malicious hackers. A good example of where this would prevent an attack from occurring is if someone were using the tool SMURF. SMURF works by attacking a system using the system's own IP address. More than likely this IP address would not fall under the ISPs "approval list" so it would not forward the packet and therefore the attack could not commence.

There is a downside to Egress filtering. It will require more Central Processing Unit (CPU) utilization of the router because now it will have to analyze each packet and compare it to a list of valid IP addresses. Therefore, bandwidth will be reduced making it an unlikely addition to many of the Internet Service Providers around the world unless their clients (you and me) start voicing our concerns.

There is also a tool being developed by Steve Gibson called Spoofarino. This tool will help users determine whether their Internet Service Provider allows spoofed IP address to be transmitted. What this will do is give you a quick and easy tool to find out if the ISP has turned on the Egress filtering feature. Once this tool is available at www.grc.com, and if enough people use it and put pressure on their ISP, we may see a decrease in the DOS attacks.

Features vs. Security – Where do we Draw the Line?

So when should we draw the line of adding features to an operating at the risk of losing some security? Or should we even be concerned about it at all? To begin with let's first look at some of the features offered as a result of full support of raw sockets in Windows XP.

- Interoperability with other Operating Systems
- Internet Connection Firewall
- IP Security Protocol
- Network Diagnostic Tools
- Gaming

(Gibson)

These are some of the main advantages added to the operating system, as stated by Microsoft in an excerpt at http://grc.com/dos/xplaughter.htm. In this same article; however, it states that full support of raw sockets is only available to administrators and not to non-privileged users. This adds some confusion to Microsoft's statements of the features. The above features are available no matter what level of user is logged in, so why then do they state you must have full access to raw socket if they work even when user's with restricted raw socket use are logged in? Please note that consumers more than likely will not use the non-privileged user option and will be viewed as "administrator" with full access to the raw socket.

Also the interoperability with other operating systems is unlike Microsoft. They operate very well with conforming to a number of other specifications that their competitors use. So again it seems that they could easily get by without including full raw socket support, yet it is there by default.

Based on the features above and the fact that they could still allow those features while limiting access to the raw socket, I believe Microsoft would do the Internet well by disabling full support of raw sockets.

As we explore the feature versus security issue further, as it relates to Windows XP, another new and exciting feature to Windows XP is one where you can actually let someone take control of your machine. This would be useful in have a friend help you troubleshoot a problem, technical support or simply accessing your machine while away. One security expert believes it will take approximately two months before malicious hackers find a way to exploit this attractive feature of WinXP. (Maiffret in McWilliams)

A final example points to scripting and email. Is there really a need for scripting in email's? Look at the number of problems this has caused and the powerful virus' that have exploited this feature. Would you say these new features outweigh the negative impact they've allowed to occur on the Internet? *(I hope some of these questions/facts help some of you think of ideas for future GSEC Practical Assignments)*

The argument for stronger features is very valid as well. Why let the malicious hacker's win and keep us from having strong and feature rich operating systems? Microsoft does have a point that if we focus on keeping malicious software off of our systems then we don't need to worry about what the operating system gives us access to. But a feature rich OS in the hands of unknowing users is asking for a world of trouble. I believe that the system should be as secure as possible by default and only when you enable options (which most beginning users will not venture towards) will you experience the full featured and more vulnerable operating system.

Conclusion

In conclusion, we should understand now that Denial of Service attacks are occurring now at a rate that is probably much higher than 4,000 per week. With the anticipated release of Windows XP in October of 2001, we will have for the first time a system that supports full access to the operating systems' raw socket right out of the box and in the hands of home users. With the ease of IP spoofing that this system will allow, the potential for a huge increase in more powerful and almost untraceable Distributed Denial of Service (DDOS) or Denial of Service attacks may become more common. While Windows XP will allow full access to raw sockets, many believe that we need to concern ourselves with not allowing iniquitous software onto the machines. Even a machine with limited raw socket access can be enabled to have full access if certain code can be executed to perform this task.

We also learned that Egress filtering can be an important tool that can be implemented on the ISP's routers to minimize the effects of DDOS or DOS attacks. Unfortunately it requires the routers to examine all data passing through it thereby reducing available bandwidth. Most ISPs do not implement this option on their routers. (Gibson)

Finally there were some questions raised that possibly others can look into regarding where to draw the line on features versus security. How far should a vendor like Microsoft go when developing their software with new features at the risk of make the system a powerful Internet attacking machine? How do we determine whether that line should exist?

Unfortunately, it will probably take a very serious situation to occur before Internet security and home based operating systems are taken more seriously. While Microsoft is taking some steps to protect iniquitous software from getting on their machines, they are also making these operating systems with capabilities that can turn them into very effective attackers if and when they are compromised. So keep your anti-virus software updated, your firewall and operating systems patched, and hope that Windows XP users do the same!

References:

1. Ploskina, Brian. "In Denial." 9 June 2001. http://www.zdnet.com/intweek/stories/news/0,4164,2783678,00.html

2. McWilliams, Brian. “New Tools Will Expose Security-Slacker ISPs.” 13 June 2001. http://www.newsbytes.com/news/01/166814.html

3. Microsoft Corporation. “Hostile Code, not the Windows XP Socket Implementation, is the Real Security Threat.” 2001. http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/itsolutions/security/news/raw_sockets.asp

4. Gibson, Steve. “Microsoft Seems to Feel that Windows XP Denial of Service Vulnerability is a Laughing Matter.” 23 July 2001. http://grc.com/dos/xplaughter.htm

5. McWilliams, Brian. “Is Windows XP a Hacker’s Dream?” 7 June 2001. http://www.sbcmag.net/texis/scripts/vnews/newspaper/+/ART/2001/06/07/3b1fd4ee9

6. Gibson, Steve. “Why Windows XP will be the Exploitation Tool of Choice for Internet Hackers Everywhere.” 19 July 2001 http://grc.com/dos/winxp.htm

Last Updated: July 24th, 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 Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
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 Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
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
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
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 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
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
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
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor