Fall 2003

PC Security in a Networked World

Joseph B. Miller
University of Kentucky, jbmiller@uky.edu

PC Security in a Networked World

PC SECURITY IN A NETWORKED WORLD

BY JOSEPH MILLER

SCHOOL OF LIBRARY AND INFORMATION SCIENCE, UNIVERSITY OF KENTUCKY

INTRODUCTION

Over the last decade, the personal computer has been transformed from an isolated word processor and number cruncher into a communications device. The emergence of the Web, the expansion of broadband connectivity, and new versions of the Windows operating system have made it possible to share information and files around the world with the click of a mouse. So, the good news is that it is now easier than ever to connect to any other host on the Internet to share information or to set up your own Internet based information services. However, this is also the bad news because it is potentially very easy for others to find and connect to your machine to set up servers there as well. Our school became painfully aware of this when we received a cheerful note from the campus computer security office informing us that there were rogue servers operating in our area that would be dropped from the network if the problem was not resolved. This paper grew out of the need to understand and deal with those attacks; it is not intended to be a review of all aspects of PC security and their Windows or network solutions, but instead hopes to increase awareness of external threats to the networked PC and to provide suggestions for detecting and deterring them. Many libraries have personnel dedicated to identifying and solving these problems, but in smaller libraries and information centers much of this responsibility falls to individuals who are not necessarily network or computer security experts. This article is directed to those non-experts operating in the Windows environment who confront these issues on a daily basis.

WINDOWS OVERVIEW

The current Windows environment (versions 2000 and XP) allows for multiple users with differing levels of access to the system. The most powerful access level is an account with administrative privileges. Administrators can set up other accounts, install programs and Internet services, and access, delete, or modify any file on the system. The TCP/IP standard (Transmission Control Protocol/Internet Protocol) that is the foundation of the Internet is now part of the operating system making remote access and control of a system possible. A suite of programs now part of Windows, the Microsoft IIS (Internet Information Services), allows one to turn any desktop machine into a server supporting various Internet protocols such as telnet, file transfer (FTP), chat (IRC), and Web (HTTP).

Any operating system has potential security holes, and Microsoft is constantly providing service packs and patches to respond to security issues as they become known. While it may appear that Windows has a disproportionately large number of such security problems, one has to keep in mind two mitigating factors: first, that it is a priority for Microsoft to make advanced features accessible to non-experts and that this goal is sometimes at odds with security concerns; and second, that the huge world-wide base of Windows systems makes them attractive targets for hackers for both practical and philosophical reasons. Because these powerful platforms are so ubiquitous and sometimes quite vulnerable, there are large numbers of hackers and virus programmers who exclusively target Windows-based systems seeking to exploit weaknesses. These hackers usually have at least one of many potentially malicious goals, including data theft, system vandalism, or rogue server operation.

TCP/IP AND PORTS

To understand how a computer can be compromised, a review of some Internet basics is called for. All the Internet protocols depend on client/server interactions. Client/server architecture is essentially two complementary pieces of software working together to either

request or deliver information, such as a telnet client talking to a telnet server, or a Web client (the browser) talking to a Web server. On the Internet, all these interactions use a packet technology known as TCP/IP (Transmission Control Protocol/Internet Protocol). Any given computer can run both client and server programs and each client/server interaction takes place through an assigned communication channel called a port. The TCP/IP specification defines 65,535 such ports! To better understand ports, think of how mail is delivered to an apartment building. The IP address of your computer is like the street address. The port used by different protocols is like the specific apartment number the mail should go to at that location. This way the same computer can receive separate streams of TCP/IP packets destined for the various client or server programs running on it. The common protocols have default port assignments, such as port 80 for HTTP. So a Web server "listens" at port 80 for client requests.

COMPUTERS UNDER ATTACK

There are really two types of attack, but they are often related. One is the completely automated attack, caused by worm and virus programs. In this case, the damage is done solely by the programs that invade the computer. However, this type of attack can frequently be the precursor to a direct, targeted attack by a hacker who wants to use that computer for their own purposes. How might such hackers get control of a networked PC? There are several approaches, and they can involve local or remote techniques. Local concerns relate primarily to the level of access someone has when they use that computer. Most users are aware that security must be high for computers in public areas; protection here depends mostly on how effectively the machine has been "locked down" by the administrator, the strength of passwords employed, and effective profile and group policy management. These settings will clearly also impact the prospects for a remote attack, but there are a number of TCP/IP related vulnerabilities that can sometimes escape our attention. Because of this, there could be many computers in physically secure environments such as offices or homes which one may naively believe are not at significant risk. So what about the remote attack on such a machine, maybe from someone halfway across the world?

Typically, the hacker first needs to identify a vulnerable machine. You might be surprised by how much information can be extracted from your computer by programs designed to just ask for it, often for legitimate reasons. Your IP (Internet Protocol) address and a list of the TCP/IP ports that are available are just two critical types of information that can be easily obtained. Once a machine has been identified as vulnerable, the next step is to gain administrative access either through guessing weak or non-existent passwords, through the use of hacking programs such as CRACK (a password decoding program), or other programs that exploit possible security holes. For instance, programs exist that can upgrade privileges of the built-in guest account to give it administrator rights or that can record passwords and send them to a remote user. As we have seen recently, Trojan horse programs, Internet worms, and other viruses can play a role in this process. Often the attack begins with a virus infection that will both identify a potential host and provide the entry point for a hacker or program. Once administrative access has been gained, the remote user can do just about anything they want; usually the goal is to set up one or more Internet services to support chat rooms with IRC (Internet Relay Chat) or FTP (File Transfer Protocol) sites for music or even pornography. The attacks that took place on our machines resulted in the creation of several such rogue servers that operated in stealth mode for some time before being detected and shut down. The security breakdowns that allow this to happen usually relate to security failures in one of three critical areas: OS (Operating System) and application maintenance, virus protection, and TCP/IP port security.

OS AND APPLICATION MAINTENANCE

Keeping the operating system up-to-date with security patches is essential and it is also one of the easiest measures to implement. Keeping up with security holes is like trying to control a leaky roof. If it is raining all the time, vigilance is called for. Not only do we have to have to minimize the damage when a leak is discovered, but ideally we'll patch potential problem areas before the water starts coming in. Microsoft updates and patches come out on a regular basis. Service Packs refer to somewhat major overhauls of the OS and might contain a large number of fixes. There is also a steady stream of specific patches to fix immediate problems. One needs to update Microsoft applications as well; Outlook, Internet Explorer and Office all have security issues to address. Users can go into Internet Explorer under the "Tools" menu option and select "Windows Update". This goes to a

Microsoft Web site[1] that can scan a system, identify critical updates, and allow one to download and install them. However, the best strategy is to automate this process. In the "Control Panel" there is an option for "Automatic Updates" where one can schedule a periodic check of a system (once a week is reasonable unless there is a specific threat announcement). However, note that administrative access to the system is needed to schedule this or to do major OS updates.

VIRUSES AND VIRUS PROTECTION

Computer viruses and worms are very common and their effects range from simple annoyance to seriously compromising a system[2]. The first line of defense is up-to-date antivirus protection. However, since most antivirus software depends on file recognition based on a definition file, one is always at risk of attack by a new virus or variant that the antivirus program hasn't seen before. To further complicate our computing life, many virus threats turn out to be hoaxes. The JDBGMGR hoax[3] is a prime example, propagated by well intended but uninformed users. An email from someone known to the user informs us that they might have infected our machine and goes on to claim that deleting the file JDBGMGR.EXE is a solution to the W32/Bugbear worm. Included in the message is the warning: "IF YOU FIND THE VIRUS IN ALL OF YOUR SYSTEMS SEND THIS MESSAGE TO ALL OF YOUR CONTACTS LOCATED IN YOUR ADDRESS BOOK BEFORE IT CAN CAUSE ANY DAMAGE." It turns out that users will always find this executable file because JDBGMGR is a legitimate Windows program (the Java debugger) and the warning we are asked to send on is a hoax.

Another source of confusion comes from programs like the Klez Worm[4] which spreads by email attachment of an executable file randomly assigned the PIF, SCR, EXE or BAT extension. It infects program files on the machine and makes changes to the registry. It then uses addresses found on the infected system to create "spoofed" email messages (i.e. messages where the TO and FROM addresses are randomly generated by the virus from addresses found on that machine) that in turn are sent out with the virus attached. Since your address may be used as the source of such a mail message FROM line, mailers that reject the message because of the attached virus will "bounce" the message back to you, the apparent sender. Receiving such a "postmaster bounce message" indicating an infected email was sent from your account causes much unneeded alarm, since in most cases, your system was not the true point of origin of the message. This problem has come up again recently with the Sobig.F worm[5].

The Nimda, Code Red, and Blaster programs, on the other hand, are potentially more dangerous. Nimda spreads in two ways: either as an attached file called README.EXE, or by infecting certain Web pages with malicious JavaScript code if the Microsoft IIS Web server is in use. Nimda[6] also attacks servers using holes left behind by a previous Troj/Code Red-II[7] attack. Nimda will try to create additional security holes such as granting administrator rights to the "guest" account, which can give a hacker full access to the system. The Code Red virus puts a copy of the program explorer.exe in the root of drive C: and makes changes to the registry which allows a hacker to issue commands and run programs on the infected machine. Once such control is gained, rogue servers can also be set up. Infection by the Blaster worm results in the downloading of a program (msblast.exe) to a system directory that will then execute. This program can cause system crashes as well as facilitate further attacks through the creation of a hidden command shell that can be exploited remotely. The worm distributes itself by scanning for IP addresses that have an available TCP port 135 and then attacking those systems.

PORT SECURITY ISSUES

As discussed earlier, TCP/IP creates many unused communication ports on your computer that are potentially available for hackers and worm programs to exploit. In addition to TCP/IP ports, another area of concern are NETBIOS (Network Basic Input/Output System) ports[8], used by Windows for certain network functions like file and print sharing. Even though many systems do not need these services, the default for many Windows setups is to enable NETBIOS through TCP/IP. These ports can then be used to provide information about your computer which can be exploited by attackers and worm programs. The NETBIOS ports 137, 138, and 139 are known as "scanner bait", because hackers and worm programs will scan for their availability and try to utilize them in their attacks. One academic institution reported that in a single day, there were over 18,000 different sources probing campus IP addresses on port 137; about half of these reflected more than 100 attempts to probe the port. They noted that a single IP address in Taiwan accounted for over 20,000

such attempts to access campus computers via port 137[9]. And as noted previously, TCP port 135 can be exploited by the Blaster worm. Unfortunately, these troubling results are not unusual and it is no wonder that many technology departments are now blocking these ports at their firewalls. You may need the NETBIOS ports to do certain types of Windows file sharing, but remember that while these ports can have legitimate functions, they also carry significant security vulnerabilities.

OVERVIEW OF AN ATTACK

So, the sequence often looks like this: First, a vulnerable machine is located, either via a virus attack or with port scanning programs. Next, a hacker may gain administrative access, either by cracking or stealing passwords, or with programs that can upgrade privileges to another account. Once this has been done, the hacker can setup server functions using the Microsoft IIS suite. These rogue server programs often are assigned an unusual TCP/IP port, given legitimate sounding names (sometimes by renaming a legitimate Windows system file), and hidden away in some system directory where they will not be easily noticed. The hacker is now ready to go into business with your machine!

WARNING SIGNS

- If a scan with your antivirus software detects a virus on your computer, go to "red alert". Do whatever is required to remove the virus and correct any changes it made to the registry. Infection by Trojan horse or worm type viruses can be a prelude to a hacker gaining full access to your computer.
- Look for unusual activity on your machine (but be sure you know what's "unusual"). This includes the sudden disappearance of free disk space; the appearance of new user accounts or folders; or a sudden, dramatic change in how long it takes a system to start up or shut down.
- If you are familiar with TCP/IP port issues, you can look for services "listening" at unusual ports, the appearance of new services like FTP or IRC, or, if it is monitored, unusual packet volume associated with that system.

Of these warning signs, one of the most important, but probably the hardest to interpret, is unusual port activity. For most users, the easiest way to check out a system is to go to one of the many Web-based security scanning sites such as Sygate[10] or Symantec[11]. These sites can scan a system and identify vulnerabilities such as high risk ports that are accessible to the outside world. For those comfortable examining their systems in more detail and interpreting the results, the "netstat" Windows command or some port scanning program like the Active Ports freeware program[12] available on the Web are useful tools to examine ports in use. To use netstat, get to a command prompt and type in "netstat -an" (the "-an" is a pair of command modifiers that provides added information from this command). These techniques can help identify unusual ports "listening" for services you have not installed. Remember that just seeing NETBIOS ports in use is not always a sign of trouble, but finding services like Telnet, FTP (File Transfer Protocol), or IRC (Internet Relay Chat) servers assigned to nonstandard ports usually indicates a system has been compromised and that appropriate remedial action is called for.

WHAT TO DO IF YOUR SYSTEM IS COMPROMISED?

First, take the suspect system off the network. Then, be sure that you do in fact have a problem. If it is confirmed that the system has been hacked, it is best to wipe the system clean and start over. Radical treatment is called for since once a system has been compromised by a hacker, just applying patches may not guarantee that the threat from that attack has been eliminated. Back up all your data files, reformat the system, and install a clean version of the operating system. After reinstalling the OS, immediately update it with all appropriate service packs and patches. Get good antivirus protection and update it. Consider the protection of a firewall at the machine level (there is one built into Windows XP and other third party products are available as well). But with local firewalls, be aware that some settings can cause unexpected problems for computers on a wide-area network. For instance, default firewall settings may not allow your computer to respond to a "ping" signal (this is when test packets are sent to an address to see if the machine is connected to the network). On some networks, responding to a ping may be required for the computer to retain the IP address assigned to it, so it is best to check local network policies before implementing a firewall.

PC SECURITY "TOP TEN LIST"

1. Use secure passwords for administrative access to the computer.
2. Implement the principle of "least privilege" – don't log in routinely as adminis-

trator; have and use a lower level account for most of your computing. Disable the guest account if it is not needed.
3. Know your machine! Have an idea of how much disk space you have available, how many user accounts are on it, who has administrative access, as well as what programs and services are installed.
4. Keep the Windows OS up-to-date with the latest patches and fixes.
5. Keep Internet Explorer and Office patches up-to-date.
6. Use Antivirus software and keep it current.
7. Consider a local firewall if it will not interfere with legitimate network functions.
8. Investigate disabling NetBIOS ports over TCP/IP and turn off the Microsoft file and print sharing features if they are not needed.
9. Learn how to check or monitor port activity with the "netstat" command, some port scanning software, or a Web-based security scan service.
10. Be informed! Know about problematic email attachments and what file extensions might indicate high risk files. Use important resources such as CERT[13] or other sources[14] to learn about common Internet hoaxes and real threats.

The networked world gives us almost unlimited access to information but that access comes with a cost. One cost is the need to be constantly vigilant and proactive in protecting the security of our personal and workplace computers. The old adage of "an ounce of prevention being worth a pound of cure" is especially true in the world of the networked PC.

Joseph Miller
(jbmiller@uky.edu)

REFERENCES

[1] Microsoft Windows Update Page, <http://v4.windowsupdate.microsoft.com/en/default.asp>

[2] Gaudin, Sharon, "The Worm that Won't Go Away." Datamation 23 Mar. 2003 <http://itmanagement.earthweb.com/secu/article.php/2084381>

[3] Sophos Antivirus Hoaxes page, accessed 2 Sept. 2003 <http://www.sophos.com/virusinfo/hoaxes/jdbgmgr.html>

[4] Sophos Antivirus Virus Analysis Klez page, accessed 2 Sept. 2003 <http://www.sophos.com/virusinfo/analyses/w32klezh.html>

[5] Nahorney, Benjamin and Atli Gudmundsson. Symantec Corporation Security Updates Sobig page. 20 Aug 2003 <http://securityresponse1.symantec.com/sarc/sarc.nsf/html/w32.sobig.f@mm.html>

[6] Sophos Antivirus Virus Analysis page, accessed 2 Sept. 2003 <http://www.sophos.com/virusinfo/analyses/w32nimdad.html>

[7] Sophos Antivirus Virus Analysis Code Red page, accessed 2 Sept. 2003 <http://www.sophos.com/virusinfo/analyses/w32codered2.html>

[8] Internet Security Systems, Inc Port Microsoft page accessed 2 Sept. 2003 <http://www.iss.net/security_center/advice/Exploits/Ports/groups/Microsoft/default.htm>

[9] "NetBIOS Blocked At Campus Border." Information Technology Services, Caltech 6 Jan. 2003 <http://www.its.caltech.edu/its/security/policies/netbios-block.shtml>

[10] Sygate Online Services Scan page accessed 2 Sept. 2003 <http://scan.sygatetech.com/>

[11] Symantec Corporation Security Check Page accessed 2 Sept. 2003 <http://www.symantec.com/securitycheck>

[12] Smartline, Inc Freeware page accessed 2 Sept. 2003 <http://www.protect-me.com/freeware.html>

[13] CERT(r) Coordination Center accessed 2 Sept. 2003<http://www.cert.org>

[14] Purportal "The Bunk Stops Here" page, accessed 2 Sept. 2003 http://www.purportal.com/