Global Information Assurance Certification Paper

Protecting the Home Network

Jim Usher

August 4, 2003

GIAC Practical Assignment

Version 1.4b

Abstract

When users connect to the internet there are inherent risks. Most users are not aware of these risks nor have they taken steps to protect themselves. This paper is intended for these users, to aid them in gaining a fundamental awareness and education of critical security issues. The focus of this paper will be around four methods of protection: Firewalls, Virus Protection, Software Patches, and File Backup.

Introduction

Many computer users were given a wake up call on August 11, 2003 when a worm named "Blaster" or "LoveSAN" was released into the wild (the Internet) infecting more than 1.4 million systems in just a few days[1].

Ironically, more than a month prior to the attack, on July 16, 2003, Microsoft announced a critical flaw in its operating systems[2]. At the same time as this announcement, Microsoft released a "Critical Update" to correct the flawed systems. Microsoft recommended that System Administrators apply the patch immediately[3]. The FBI[4] and the U.S. Department of Homeland Security[5] issued an advisory on July 24, 2003 as well, detailing the flaw and again recommending updating the affected systems.

Many users and System Administrators undoubtedly read or heard about this flaw, but ignored it and the potential impact on their systems. It could be expected that many home computer users would not know about nor pay attention to the announcement by Microsoft, but what about major corporations? Yes, major corporations were infected as well! Even though these large corporations were protected by layers of defense like a firewall, they failed to heed the warnings from the above mentioned sources and did not update their systems and were subsequently impacted by the worm. This worm proliferated so effectively that,

> It forced Maryland's motor vehicle agency to close for the day and kicked Swedish Internet users offline as it spread, its instruction set triggering Windows computers to shut down and restart[6].

Usually a user will not take the time to set up a strong defense unless their system has been knowingly compromised. If the user has been compromised without any noticeable impact, the user will have no incentive to take action. When asked, some users indicated that they did not think their computer system was infected because it was working fine. In cases where there is no security defense, there is a high probability that these systems have already been infected. According to viruslist.com there are about 53 active viruses "in the wild" today [7].

It is this authors hope that this latest worm will have the effect of making more computer users aware of the risks associated with being a member of the global

internet community. Each user has a right and a responsibility to set up security defenses. If they don't, we will continue to have world wide spreading of threats such as this worm.

The good news is that Internet users can protect themselves by following just a few steps. There is no single method of protection that will insure complete safety from hacker activity. However having a multi-layer approach to internet security will protect the average home user from most threats. This latest worm will frequently be used to demonstrate how performing these steps would have protected a home user from being compromised. Firewalls, Anti-Virus software, Patch Updates, and Backups will be discussed as layers of defense. The reader will be shown how implementing only one of these steps will still leave a potential vulnerability open, but implementing all of these steps together will provide the needed protection from this specific threat and many other threats.

This author also feels strongly that Ad-Ware / Spy-Ware scanning and removal should be implemented into Anti-Virus software, but currently it is not. We will also discuss this topic to bring an awareness of this little known issue to the user. There are many other behaviors and actions a user can and should do to protect themselves on the internet. This paper will not delve into these steps. However, references are provided at the end of this document.

IP and Ports

Before we can discuss improving security, some Internet basics must be covered. First of all, each and every computer connected to the internet must have an IP address. This is like a telephone number for a computer. When a computer connects to another computer on the internet it "dials" that computer and lets that computer know who called (caller id) – their IP address. By the way, when a user really does dial up to the internet their ISP provider is providing a connection that ultimately provides an IP address to that computer. There is much more to this but this is the basic concept. For each IP address there is another concept called "ports". Imagine the phone as having several different rings. When the phone rings and the fax machine hears its specific ring then the fax machine picks up. If the Answer machine ring comes through then the answer machine picks up, and so on. It just so happens that computers have 65535 of these ports. In the internet world something that answers on a port is called a service. Examples of services could be a web server (port 80 and/or 443), FTP (21), Mail 25, etc.

Hackers and port scanning

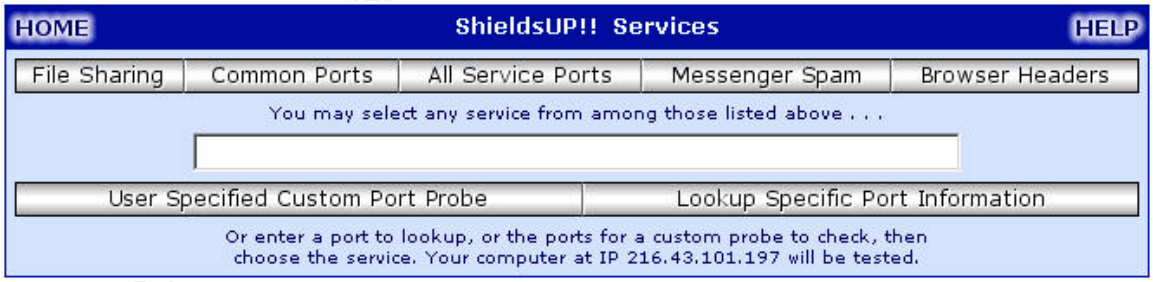
The Blaster worm was written with the specific intent to exercise a flaw in Microsoft's latest operating systems. This flaw left a vulnerable service running on port 135. The worm was created to scan for this port. This means, try random IP address on this specific port. If the port is inaccessible then the worm ignores that IP and moves on. Any user having this port turned off or not even there

would mean their computer could not be attacked by this worm. Hackers can also scan directly for open ports. If a computer is directly exposed to the internet there will be several ports open by default. Based on which ports are open and how the computer responds on these ports the hacker can tell which operating system is actually running on that computer. There are many web sites on the internet that detail what vulnerabilities have been found for which operating systems, the hacker only has to attempt to exercise the particular vulnerability. If successful, the hacker can browse the user's system, monitor activity including passwords, download account numbers or files, pretty much anything. The hacker will take basic steps to insure that the user does not even know that the compromise has occurred. This is called a "stealth attack".

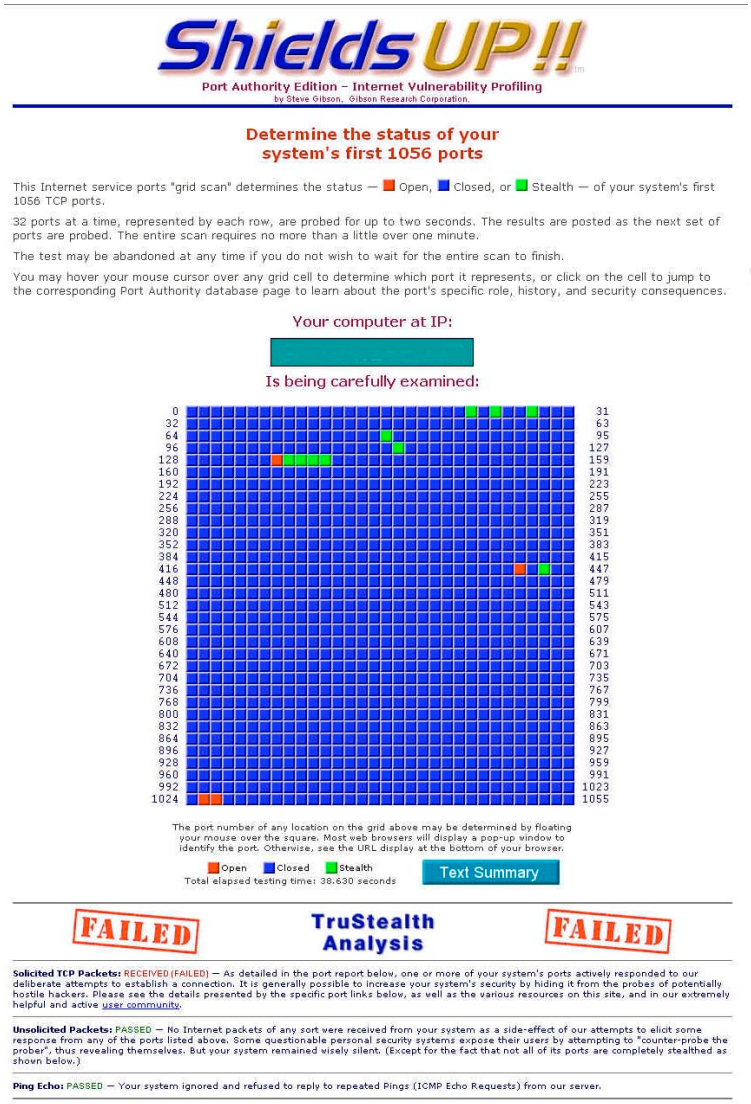
In an attempt to make a home network disappear from the hacker's radar screen, users should not only know about port scanning, but actually perform a port scan on their own systems and take steps to hide their machine from such attempts. Below is one method of accomplishing this.

A port can be in one of three different states, Open, Closed and no-response or Stealth. The user could download a port scanning utility and attempt to scan their own computer but this test would not be a true view of their system as seen by a hacker or a worm on the public internet. The only true test is to scan the users IP address from the public internet. The easiest way to do this is to use the "Shields Up"[8] website. Through this web site, the user can have the first 1055 ports scanned and a report will be generated indicating which ports are open and at risk. Using this site the user can also scan just the most common ports, or actually specify a specific port to scan. To do this, follow these steps.

1. Browse to https://grc.com/x/ne.dll?bh0bkyd2
2. Towards the bottom of the screen, click on "All Service Ports" button.



3. A page similar to the following should slowly appear.



When the user first contacted the website the IP address used was recorded. If a NAT Router/Firewall is used, this would be the internet IP not the actual LAN IP address. While this page is painting the Shields UP server is attempting to probe the users IP at each and every port from 1 to 1055 recording each response. On the graph a Blue block indicates that port returned “I am here but I am not providing this service at this time” or in other words - “closed”. A Red block indicates that this port is “Open” for business and can be attacked from the internet. A Green block means that the machine at this IP address did not return any response for this port – “Stealth”.

The goal from a security standpoint is to have all ports be Green - “Stealth”. If a port reports itself as open (red) or even closed (blue) a hacker would know that the computer is there and that it might be worth looking into. The best response

is no response at all (Green). This way the hacker would assume there is no computer at that IP address and move on to the next target.

The above scan clearly shows that the machine used is responding on all but a few ports, even though most are “closed” (blue). A few ports are actually open (red) and ready to be exploited. In the next section we will describe firewalls and how to “Stealth” all ports and get a “Passing” (completely green) grade from the Shields Up utility.

Firewalls

The author of the Shields Up web site describes a firewall in the following manner.

> A firewall ABSOLUTELY ISOLATES your computer from the Internet using a "wall of code" that inspects each individual "packet" of data as it arrives at either side of the firewall — inbound to or outbound from your computer — to determine whether it should be allowed to pass or be blocked[9].

Generally, a firewall is configurable, defining rules that instruct the firewall how to either allow or block traffic. A firewall can be either a physical piece of hardware or a piece of software. Most commercial firewalls are so sophisticated that they are able to define specific rules that instruct the firewall to allow or deny certain traffic, based on either the source or destination IP and/or port. For example, a rule could be defined as “allow web traffic on port 80 into this network from any IP in the range of 198.60.146.*”. This is very powerful and provides a lot of control and protection for the network. These types of firewalls may be purchased in the private sector, but most users would feel this is too complicated and they truly do not have the level of need a large corporation would have. Instead, most consumer level firewalls are less sophisticated, yet provide a strong level of protection.

Physical Firewalls

A physical firewall would be some network device that sits between the user’s internet connection (Cable Modem) and the computer resources it is protecting. Most devices for the consumer also have additional features like DHCP, HUB/Switching which are nice to have and simplify the setup of a network. One example of such a device is the Linksys EtherFast® Cable/DSL Router with a 4-Port Switch[10]. This product costs only about $60 at CompUSA[11]. To be clear this device is NOT a full feature Firewall. For most consumers however this device will provide the needed level of security.

The difference between a NAT Router and a true firewall is that the NAT router is able to know where a connection was initiated from, either the inside of its network or outside (the internet). If the connection was initiated from the internet, the traffic will be ignored or “stealth”. If the traffic was initiated from inside the network the router performs a nice function called NAT - Network Address Translation. This means that the user’s computer may have an IP address of 10.0.0.1, but when the router gets the request, it converts it to the IP the router was given by the ISP, say 145.60.123.78. This last IP address is what other users and servers will see. Also, the router can provide this NAT function for up to 253 computers. The home user can subscribe to an ISP and be assigned a single IP address, have a home network consisting of 1 to 253 users all using the same single ISP connection and the same external IP address and every

computer on the network can have access to the internet and the other computes on the local network. Using a NAT Router configuration in this way also provides a layer of protection that prevents a hacker from ever being able to directly connect to any one of these machines. That is a one time cost that will protect all computers on the network now and in the future. Please note, the router mentioned above is able to handle 253 computers and provide internal IP addresses for each but the device itself only comes with connections to support 4 computers. If additional computers are needed on the network additional hubs and/or switches would be necessary.

This NAT Router prevents direct attacks from the internet, but does nothing to protect any user inside the Local Area Network from downloading malicious code (worms, virus', Trojan horse, etc.) which then propagates itself within the network and out again into the internet. This firewall will also not protect the users if those users install peer to peer network software like Kazaa[12].

Port 113

Some users may notice that even though they have a NAT Router in front of their network, they still have a single port that is reporting as closed, instead of "Stealth" – port 113. This port, for the most part, is no longer used. However the NAT router manufactures did not want to stealth this port since someone might actually need the service so they report it by default as "closed". If you are trying to have all of your ports respond as "Stealth", then this is unacceptable. There is a simple way to configure the Router so that this port is also "Stealth". The basic version of how to do this is to configure the router so that it forwards all traffic destined for port 113 to a non-existent machine[13]. By doing this, any attempts to access this port will result in no response and the IP used will PASS the Shields UP test.

Personal Firewalls

If there is only 1 computer that is connecting to the internet either by using a dial up or a high speed connection such as DSL or Cable, a Personal Firewall may be a better fit. A personal firewall is software that is able to protect a machine once installed. This software analyzes the information from the network prior to the computer actually performing any action on it. This way this traffic can be blocked or allowed depending on how the firewall software is configured. Again this software will only protect information coming into and out of this specific computer. In some ways this is better. If this computer is on a LAN and another computer has been infected with a worm (such as MSBLASTER), that worm will try to connect all machines near it on the local network, when the target machine is the one protected by the personal firewall the firewall will deny all attempts from the worm and therefore successfully protect the machine. Most Personal firewalls come with additional features like script blocking, and application level allow/deny rule sets for network access. This last feature is to prevent an unauthorized program (like a worm or a Trojan horse) from accessing the

network. This is done by prompting the user anytime a program attempts to access the network. The user is then responsible for knowing what the program is and whether or not access should be granted. Most users will find this annoying and would not know if a specific program is malicious or not. Therefore they would either allow all access or get so frustrated with the constant promptings that they would consider uninstalling the product or disabling this feature. This is a nice feature and the user should consider spending the time to understand what programs should be allowed to access the network based on the users own actions.

Cost of these types of products range from free to around $50. Here are some providers of this software (in no specific order);

1. Zone Labs – ZoneAlarm Pro[14]
2. Tiny Firewall 5.0[15]
3. McAfee Security[16]
4. Symantic[17]
5. Windows XP also comes with a built in firewall that will perform basic blocking[18].

Which configuration to use?

There are many different types of configurations home users can set up, but most of them will decide 1 of the following 3 options.

1. Not install any firewall (not recommended)
2. Install a NAT router
3. Install a Personal Firewall.

The following sample situations and their recommended configuration have been provided below to aid the user in the decision making process.

Situation #1: High-speed dedicated connection and have now and will only have one computer.

> Either a **Personal Firewall** or a **NAT Router / Physical Firewall** could be used. Since only one machine is needed to be protected the Personal Firewall may be the better choice due to the fact that it provides more security features than the router.

Situation #2: High-speed dedicated connection – such as Cable or DSL and will have multiple computers and NO services will be provided to the internet.

> **NAT Router / Physical Firewall** should be used. In this way all computers in the LAN will benefit from the properly configured Router/Firewall.

Situation #3: High-speed dedicated connection, have or will have multiple computers on a LAN, at least one of which WILL provide a service to the internet such as a web or an FTP server.

> **Both** should be used. The **NAT Router / Physical Firewall** will provide general protection to the entire network. However, the **NAT Router / Physical Firewall** will need to be configured to forward all of the required traffic (port 80, 21, etc) to the appropriate machine within the network. This will make this IP address a potential target since a port scan will reveal this service. Therefore, it is recommended that a **Personal Firewall** also be installed on any machine providing a service. By doing this an extra layer of defense is created that further protects this computing environment. At a minimum, do not install a NAT Router and install **Personal Firewall** on each computer on the network.

Situation #4: Dial on demand (Dial-up) ISP connection for one computer.

> **Personal Firewall** should be used. There are products available that could act as a physical firewall for dial-up, but most users would not take the time to research these, configure, or pay the cost to purchase these. A personal firewall provides a strong level of defense for the single machine.

If a home user that had been attacked by the Blaster worm, had a firewall installed, they most likely would not have been infected. Again, the Blaster worm proliferated throughout the internet by scanning random IP addresses on a specific port. If a machine was found with this port open, the worm attempted to exploit the vulnerability and infect the target machine. Firewalls are designed to specifically stop unwanted traffic to the entire network. Had this been in place at the time the worm was scanning for potential targets, the firewall would have not responded, the worm would have moved to the next address. This is just one layer of defense but a very critical one. Any user that has a machine connected to the internet WITHOUT a firewall is putting their computing resources at a great risk as evident by the effects of the Blaster worm. There are other threats that are much more damaging than this worm, but this is a topic outside the scope of this paper. Another line of defense that could have prevented the Blaster worm from infecting a machine is Virus Protection which will be discussed next.

Anti-Virus Programs

Many corporations, even large corporations, have commercial grade firewalls in place and yet users on these networks were still attacked. This is a great example that any single defense is not sufficient to provide a complete defense or "defense in depth".

In the above situation, most likely the firewall was successful in blocking the worm from attacking from the internet. However the users connect to the network in several different ways. A scenario as simple as a user with a cable modem at home (no firewall) becomes infected with the worm, takes laptop to work and connects to the network and begins infecting all machines connected to same network. The firewall was not effective in this situation because the distribution was not from the internet into the company, which is the purpose of the firewall, but rather, it was from inside the company to the rest of the company. This is called a "Behind the Wall" attack. If each machine had a Personal Firewall running on it, they would not have been attacked. In most large installations this would be a large administrative challenge and cost prohibitive. Another method of solving this threat would be to have each machine run a copy of Anti-Virus software.

The purpose of anti-virus software is to defend the machine against known malicious software. It does this by performing scans of memory, boot sectors on disk, files on disk and many others depending on the vendor. The anti-virus companies are constantly keeping up to date on the latest threats to computers, whether they are in the form of a virus, worm, Trojan horse, macros, scripts, etc. When a new threat is identified the vendor performs a threat assessment and defines how to repair the damage, once a machine has been compromised. This "correction" is compiled into a virus definition file. This file is then made available on the internet so that each subscribed user can download it, thereby enabling each user's copy of the anti-virus software to be able to "scan" for and "clean" the user's machine of any possible infection. Most software will require a "subscription" which is stated in terms of some time period usually years. This is necessary since the user is buying more than just the software; they are buying a service, a service to keep the virus definitions up to date.

Many users believe that they have not been infected and won't be infected; therefore, they do not need to purchase anti-virus software. These same users would quickly change their mind if their machine was infected just once with a virus that wiped their hard drive, or scanned their email address book and sent a "not so nice" email to all their friends and family, or enabled a hacker to scan their machine for credit card numbers. Many users have a worm, virus or some other malicious software on their machines and don't even know it. Not all threatening software is noticeable. In fact most Trojan horse programs prefer to go unnoticed so that the hacker can continue to use the compromised machine.

Here are some of the most popular anti-virus software products (in no order).

1. Trend Micro – PC-cillin[20]
2. Zone Labs – ZoneAlarm Pro[21]
3. McAffee Security – Virus Scan Home Edition 7.0[22]

Once the software has been purchased, installed and virus definitions updated a full system scan must be performed so that the system can identify if there are currently any threats on the machine at the time of installation.

Here is an example of the detection of a worm.

This particular worm had found its way into a subdirectory of a web tree. We have discussed worms and viruses frequently. By now the reader may be wondering why there is a distinction, “Aren’t these the same thing?” Technically, they are different; they have several similarities, but have one primary difference. That difference is that once a virus has been delivered, it must be executed by the user, a worm does not. Once launched, a worm will propagate itself through the internet without any intervention by any user. A virus is typically emailed, transmitted via removable media such as a floppy disk, or is copied using network shares. In each of these cases the user would have to execute the infected file in order for the virus to continue to infect.

After a scan most products will automatically correct any infected file. Depending on the virus the file might be able to be “cleaned” or repaired. This would restore the file to its original state. However if the file can not be repaired it will be deleted as in the above example.

Consider that if the user had only 1 line of defense, anti-virus software, they may still have been attacked by the Blaster worm. For example, if a worm is launched on Friday (usually this is the case) and the attack happens to hit the target machine that evening, the virus definitions have probably not been updated or defined regarding this specific worm – the target system is infected.

This is another point for defense in depth. No single defense can defend a system properly. It takes many layers to reduce risk of compromise.

Continuing the above scenario, the anti-virus software vendor discovers the worm over the weekend analyzes it and publishes the new virus definition. The user's anti-virus software downloads the update. With the new virus definition the system automatically scans for any infected files, discovers the worm and "cleans" it from the system. Most vendor programs default their systems to NOT auto-update the virus-definitions. For the above reason it is recommended that auto update be turned on.

Some vendors provide "Heuristic protection". This means that even though a specific virus definition does not exist, a worm or virus may still not be able to penetrate this software's protection. In other words, the program is intelligent; it knows the behavior of malicious programs and attempts to stop them from infecting the protected machine. This is not 100% effective, but again, it is another layer of defense.

Email is the biggest culprit of virus transmission these days. Again, viruses need the user to execute the infected file in order for the virus to prorogate. This is why most security policies include steps to protect users from executing potentially dangerous email attachments. Users should never execute an attachment that they were not expecting or was delivered from an unknown address. Most anti-virus software will scan all email attachments in or out of the machine for viruses. This provides another layer of defense.

There is another category of software that should be noted, Adware and Spyware. These are programs that are inadvertently downloaded with some other program. These programs do not perform any damage to the machine; however, they do present a risk to the confidentiality of the user. These programs are used by marketing companies to monitor the web browsing behaviors of the user. They also can cause the users machine to reset the home page, force advertisements into web browser pop up windows, etc. This type of activity should be given the same consideration that virus' and worms are given. However, since these programs are not necessarily malicious in nature they are not scanned for or by anti-virus programs. Lavasoft's Ad-Aware[23] and SpyKiller[24] are able to scan for this type activity. There are free versions of each. This software works very similar to anti-virus software in that you must frequently download new update files and scan often. If the user has ever downloaded freeware or multi-media from the internet, there is a strong possibility that there is some adware or spyware running the machine. The free version will allow the user to download updates (new definitions), but will not protect them from receiving the programs in the first place. To have the program scan the system automatically and in real time, a licensed version is required.

So far, we have discussed two layers of defense for the typical home user, firewalls and anti-virus software. Even with these two strong defenses in place there is still a risk of being infected by the blaster worm. Example: Worm

presented behind the firewall and virus definitions not in place quick enough. The next defensive step that is needed is applying Software patches.

Applying System Update Patches

If Chevrolet were to announce that "all owners of a Silverado truck manufactured in 2002 or later can go to any dealer and will receive free upgrades to their truck to the latest standards", how many people would take advantage of such an offer? Just about everyone right? This is what most large software vendors do. In fact most even provide a convenient mechanism for doing so. In Microsoft's initial announcement about the vulnerability[2] the reader was informed that a patch was available, a link was also provided to aid the user in getting and applying the update. Even so, many Administrators did not take heed to the warning and ended up being directly infected by the worm. Had this update been applied, the worm would not have been able to infect the updated machines. For most, the update would have taken only a few minutes. After being infected by the worm, these administrators and users were forced to take the time to repair their system. Much more time than if it had been updated shortly after the announcement.

The user should check for an update for each piece of software that is being used. This may include the following.

1. Microsoft Windows – http://windowsupdate.microsoft.com
   Critical updates should be considered required updates – everything else is at the users' discretion.
2. Microsoft Office - http://office.microsoft.com/productupdates/
3. Virus Definitions and program files – see vendor's website.
4. NAT Router firmware. This is not required, but is a strong recommendation. http://www.linksys.com/download/firmware.asp?fwid=3

Backup of critical data

The last layer of defense is preventative in nature. Assuming the worst case scenario of a complete system failure, the user will want to be able to recover their machine and return that machine to pre-failure run state. This can only be done if there are backups. There are many strategies for backing up a machine. The most complete of these would include making a complete backup weekly and a daily incremental backup. Most users do not have a tape backup system and do not plan on buying one. Writeable CDs (CDR and CDRW's) are now becoming standard in most machines and blank CDR's are becoming very cheap (about $10 for 50). Each of the CD's can contain between 650-700MB of data. A simpler backup approach is to have the user identify all of the user data that would be required in a restore operation. Most backup systems will backup the entire system, the operating system, programs, data files, everything. Most of this

information is already backed up in the sense that the user still has the original media. If a catastrophic failure does occur the user could bring the fixed system up from a newly formatted hard drive, reinstalling the OS, and applications. The only missing piece left is the data the user created; documents, spreadsheets, pictures, drawings, music, etc. If the user kept this data in a single folder – like "My documents" or "AmysStuff" then they could easily copy this directory to a CDR and maintain this as a backup. Then when restoring the system the user would simply copy the directory from the CD to the hard drive, and be up and running with only minor effort. Since this backup CD will likely contain personal information, be sure to destroy any CD's prior to throwing them away.

Conclusion

The Blaster worm is a recent example of how vulnerable users (and corporations) are today. We live in a great era of technology, but this has not come without risks. The Blaster worm was fairly non-destructive. The creator of this worm clearly intended to make a point rather than to harm computer resources. They just as easily could have written the worm to reboot and reformat the hard drive – or simply delete critical files from the hard drive; pretty much anything they wanted the machine to do.

This paper has discussed four steps to securing the home network.

1. Install a firewall – Personal or Physical
2. Install Anti-Virus software
3. Keep all software up to date – If nothing else – keep the operating system up to date.
4. Make backups – Maybe the user will never be infected by a malicious worm, but the odds are good that the hard drive will fail at some point. Without a backup, there is NO recovery.

These four steps will greatly improve the overall security of the user's computer, but there are additional steps that the user should research and take. One of the most important themes of this paper is that not one of these solutions alone provides the needed perimeter of defense. Each layer that is added increases the strength of the overall security architecture.

References

1. See Appendix 1-2.
2. Microsoft's initial bulletin detailing vulnerability: http://www.microsoft.com/security/security_bulletins/ms03-026.asp
3. Post Blaster worm attack – Microsoft's info and how to resolve: http://www.microsoft.com/security/incident/blast.asp
4. FBI Urges Microsoft Windows Users to Update http://www.infosecnews.com/sgold/news/2003/08/06_01.htm
5. U.S. Department of Homeland Security advisory http://www.nipc.gov/warnings/advisories/2003/2nd%20Update8122003.htm
6. Warnings did little to stop latest computer outbreak, Anick Jesdanun, The Associated Press - http://www.securityfocus.com/news/6710
7. Virus Lilst - http://www.viruslist.com/eng/viruscalendar.html?mmonth=8&mday=13&wday=3
8. Shields Up Utility - https://grc.com/x/ne.dll?bh0bkyd2
9. Firewall Definition - http://grc.com/su-firewalls.htm
10. Linksys Etherfast Cable / DSL Router - http://www.linksys.com/products/product.asp?grid=34&scid=29&prid=20
11. Compusa - Router price - http://www.compusa.com/products/product_info.asp?product_code=273755
12. Kazaa - http://www.kazaa.com/us/index.htm
13. Shields Up – Stealthing Port 113 - https://grc.com/port_113.htm
14. Zone Labs – ZoneAlarm Pro - http://www.zonelabs.com/store/application?namespace=zls_main&origin=global.jsp&event=link.catalogHome&&zl_catalog_view_id=201&lid=nav_ho
15. Tiny Firewall 5.0 - http://www.tinysoftware.com/home/tiny2?s=215368394722265327 5A0&la=EN&va=&pg=tpf5-news
16. McAfee Security - http://us.mcafee.com/root/package.asp?pkgid=101&WWW_URL=www.mcafee.com/myapps/firewall/
17. Symantic - http://www.symantec.com/sabu/nis/npf/
18. Windows XP – Firewall - http://www.microsoft.com/windowsxp/pro/using/howto/networking/icf.asp

19. Virus definition - http://www.cit.cornell.edu/computer/security/virus/seminar-june02/immunity/sld004.htm
20. Trend Micro – PC-cillin - http://www.trendmicro.com/en/products/desktop/pc-cillin/evaluate/overview.htm
21. Zone Labs – ZoneAlarm Pro – http://www.zonelabs.com/store/application?zl_catalog_view_id=201
22. McAffee Security – Virus Scan Home Edition 7.0 - http://us.mcafee.com/root/product.asp?productid=vs7
23. Lavasoft – Ad-Aware - http://www.lavasoftusa.com/software/adaware/
24. SpyKiller - http://www.spykiller.com/

Other useful links

- CERT Coordination Center, Software Engineering Institute, Carnegie Mellon Univeristy http://www.cert.org/homeusers/HomeComputerSecurity
- CERT Coordination Center – Home Network Security http://www.cert.org/tech_tips/home_networks.html
- Intel Technology Journal – Home Network Security http://cedar.intel.com/cgi-bin/ids.dll/content/content.jsp?cntKey=Generic+Editorial%3a%3asecurity_home_network&cntType=IDS_EDITORIAL
- U.S. Department of Homeland Security – Seven Simple Computer Security Tips http://www.nipc.gov/warnings/computertips.htm
- Common Sense Guide for Home and Individual Users http://www.isalliance.org/resources/papers/ISAhomeuser.pdf
- Trend Micro - WORM_MSBLAST.A definition - http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MSBLAST.A
- Symantec - W32.Blaster.Worm definition - http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html
- Carnegie Mellon - CERT® Advisory CA-2003-20 W32/Blaster worm - http://www.cert.org/advisories/CA-2003-20.html
- Computer Security Resource Center (CSRC) http://csrc.nist.gov/pcig/cig.html/winxp-checklist-121902.doc

Appendix

1-1 SANS NewsBites Alert of Vulnerability

SANS NewsBites July 23, 2003 Vol. 5, Num. 29

FLASH ALERT

The first story below describes a critical Microsoft vulnerability (MS03-026) that affects Windows NT, Windows 2000, Windows 2003 Server, and Windows XP. A worm using this vulnerability would find more than ten times as many potential victims as Code Red. If an efficient worm is launched, so many infected systems will be searching for victims that you will not be able to download the patches before being infected. Do *not* rely entirely on blocking traffic to port 135 as a defense. Install the patches. If you needed a reason to launch a sweeping vulnerability elimination program on all Windows systems -- including the home computers from which your users connect to your corporate systems -- this is it.

Alan

TOP OF THE NEWS

--Microsoft Warns of Critical Flaw

Microsoft announced a critical flaw in most Windows systems, including Windows 2003 Server, the first system to be built entirely under the Trusted Computing Initiative (TCI). The flaw allows attackers to take over the victim's computer and install and run malicious code. In response, some users questioned the value of Microsoft's Trusted Computing Initiative.

http://www.computerworld.com/securitytopics/security/holes/story/0,10801,83130,00.html

http://www.computerworld.com/securitytopics/security/story/0,10801,83221,00.html

Microsoft Bulletin:

http://www.microsoft.com/security/security_bulletins/ms03-026.asp

CERT Bulletin updated Monday:

http://www.cert.org/advisories/CA-2003-16.html

Editor's Note (Schultz): Critics of the TCI should recall the number of vulnerabilities that surfaced in the first few months after the release of previous Windows products such as Windows NT and Windows 2000. The current number of vulnerabilities in Windows Server 2003 pales in comparison.]

1-2 SANS NewsBite announcement of Worm progress

SANS NewsBites August 13, 2003 Vol. 5, Num. 32
TOP OF THE NEWS

--Windows Worm Spreading

(11 August 2003)

A worm that exploits the widespread Windows RPC DCOM vulnerability is spreading quickly, according to the Internet Storm Center. Alternately called "Blaster" and "LovSan," the worm infects Windows 2000 and Windows XP systems and often causes them to repeatedly crash. SANS Internet Storm Center issued one of the earliest advisories about the worm. As many as 1.4 million systems have been infected as of 4 PM EDT, Tuesday. That is at least four times the number infected by Code Red.

http://www.washingtonpost.com/wp-dyn/articles/A46233-2003Aug11.html

Useful "How-To" for cleaning it off your system:

http://www.washingtonpost.com/wp-dyn/articles/A49251-2003Aug12.html

Technical description at SANS Internet Storm Center:

http://isc.sans.org/diary.html?date=2003-08-11

http://news.com.com/2102-1002_3-5062364.html?tag=ni_print

http://www.cert.org/advisories/CA-2003-20.html