Global Information Assurance Certification Paper

Basic Securing of a Charity or Small Business for Free or Low Cost

GIAC Security Essentials Certification (GSEC)
Practical Assignment

Submitted by: Corey Phillips

Date Submitted: February 24, 2004

Version 1.4b (amended August 29, 2002) Option 1

Abstract

In this paper, I will describe how to protect your charity or small business against the most basic of information warfare threats while not spending a lot of money nor being a security expert. All the items in this paper a person comfortable using a computer should be able to complete. You will end up with a system that has deployed decisive layered security that should be considered the very minimum for conducting business online. To do this I will cover Antivirus Solutions, Firewall(s), System Patching, Policy Communication & Enforcement, Disaster Planning, and using Free/Open Source Tools to help audit along the way.

This paper is not intended for an organization that is connected to the Internet and is allowing external (Internet, Extranet or clients) resources to directly access internal resources. I will be focusing on an organization that likely has an Internet Service Provider provide their email services and they use the Internet as an electronic resource (web searching, communications etc.) which is outward going to the Internet only.

Table of Contents

Information Security is an issue that affects large and small organizations alike. A large organization will typically have dedicated people, budget, time and technology to ensure that they are reasonably secure. Small organizations however do not have these resources available to secure themselves but it is just as important to try and be as secure. As a charity check with the commercial software vendors to see if special "charity" pricing exists. Microsoft offers Charity Open License pricing which greatly reduces the cost of ownership but allows the use of current technologies.

This task can seem daunting to the lone system administrator, company owner or secretary who happens to sit closest to the server. It is important to realize that no system is 100% secure. This is especially true for companies connected to the Internet. This is not to be considered an exhaustive list of inexpensive things to do, just the basics to building security in depth for a small organization. This paper also assumes that your organization is connected to the Internet but is not hosting externally available services (for example you are not running an e-business site selling on the Internet directly making money from the Internet).

As the person looking after security for your organization you should understand what you are trying to protect and what threatens it. The information that your company considers proprietary, confidential and secret must be protected. Your company can be held liable for what your computers are doing while connected to the Internet. There are the obvious things that you need to make sure that your systems are not engaged in (hacking, surfing child porn etc.) but there are also the not so obvious (your machine was used in a Denial of Service attack on another corporation due to insufficient patching – you company did not exhibit due diligence.)

The areas to cover in securing your organization should start with an adequate Antivirus Solution, Firewall(s), System Patching, Policy Communication & Enforcement, Disaster Recovery, and using Free/Open Source Tools to help audit along the way. By doing this you build layers that a would-be hacker needs to tear down before they can get to the next level. Hopefully this will discourage them so that they look for an easier target to compromise.

The first place to start is sort of a chicken and egg scenario. Let me explain. If you go on the Internet without properly firewalling your system you will be susceptible to known operating system vulnerabilities, port scans etc. If you don't have installed an antiviral package you will be susceptible to worms/Trojans that are ever present on the Internet. (It could be argued that patching should be included in this initial step before going online. Unfortunately most cumulative operating system patches are found online and can take a significant amount of time to download. Virus definitions and software firewalls are generally small in comparison to a service pack. Service Pack 4 for Windows 2000 is 132 Megabytes in size). A long download time translates to potential compromise of your system.

What is for sure if you don't do both of these you are leaving your system at great risk. It

is ideal if you can get both antivirus and firewall patches installed from clean media, downloaded from a known clean machine instead of having to go online to do the updates. For this discussion I will start with antiviral software as the starting point.

Antivirus Software

The antivirus software is to help prevent the intrusion of unauthorized software or malware to your system that usually comes though to your system through legitimate means (like a floppy, CDROM, or email message). It should be noted that layered security dictates that you should run the antivirus software on all systems, gateways and servers in a network. In the past it has been a nuisance when your machine has been contaminated with a virus. With the newer worms and Trojans it is possible for a third party to control your system, launch a denial of service attack or trash your server all from the comfort of their home.

There are many manufacturers of Antivirus software. Some will even bundle in a package an antivirus package and firewall together. Commercially available packages will generally have media that you can do a base install from to give you a starting point. It will be extremely important that one of the first things you do online is update this software. Most packages today have an online update facility that you can download the antiviral database to update your product with out having to download the whole package again.

One thing to watch when purchasing a boxed (retail) antivirus package is to make sure that the CD is not more than a few months old (I went to Symantec's web site (http://securityresponse.symantec.com/avcenter/vinfodb.html) and counted over 60 new virus threats that have been found this month. If the software was 6 months old you could surmise that there were 60 time 6 threats that the software is not aware of). If the CD is older than that then it is stale stock and should be avoided as it will take longer to update the antiviral databases when online and the increase of time to download will make you susceptible to infection during the download time. If you find that you have an older CD that you are installing from it is wise to download the updates to a known virus/worm free computer and copy the updates to the new machine so you can apply the updates before going online. To see a list of anti-virus solutions please refer to Appendix A with vendor pricing at the time of writing.

One thing to remember when setting up antiviral software is that you need to use the scheduled update functionality in the software to make sure that you are able to fight the latest virus or worms. How often you schedule a download will depend on Internet connection speed and other variables. With the time from initial release of a vulnerability to release of a virus that attacks the vulnerability decreasing every day, I would recommend having virus definitions updated at least once a week, once daily would be preferred.

Firewalls

A firewall is a device or software that separates friendly networks (your LAN) from unfriendly networks (Internet, Customers, Suppliers, Extranets etc.).

It should be noted that firewalls come in both hardware and software versions. Both have their place in small organizations.

The hardware firewall is good to deploy between your network and the Internet. It provides perimeter security through Network Address Translation (NAT), and the filtering of what IP addresses & ports are allowed into your trusted (internal network). I would recommend a firewall that is capable of Stateful Packet Inspection. One that can protect against Ping of Death, SYN Floods, IP Spoofing and other Denial of Service attacks is highly recommended also.

In the security realm if something is not needed then it should not be enabled or if possible not installed at all. With a firewall this is a rule that firewall administrators live by. If you don't have a need to pass WEB traffic inbound then there shouldn't be a rule allowing inbound WEB traffic. That also goes for quite a few home applications that make their way to a charities desktop. I would highly recommend blocking access to the ports that peer-to-peer networks like Kazaa and Chat groups use. These types of services are known for being laden with viruses and also can contain unwanted content.

Inexpensive hardware firewalls are cropping up in all kinds of devices. A software or personal firewall in the small corporation can be deployed at the desktop/server level as well. It should be noted that some of the large firewall vendors are starting to sit up and take notes on what the desktop firewalls are doing. Checkpoint Software has recently announced that they will be acquiring Zonelabs. This acquisition of Checkpoints is legitimizing the personal firewall for more than just home use.

You might ask why you should deploy a firewall at the desktop level when you have a perimeter firewall. The reason is that the desktop firewall can catch things that may seem like legitimate traffic that your firewall would normally pass through. A good example is the Welchia Worm that circulated in September 2003. This worm did several things but a personal firewall configured correctly would have alerted you to the following:

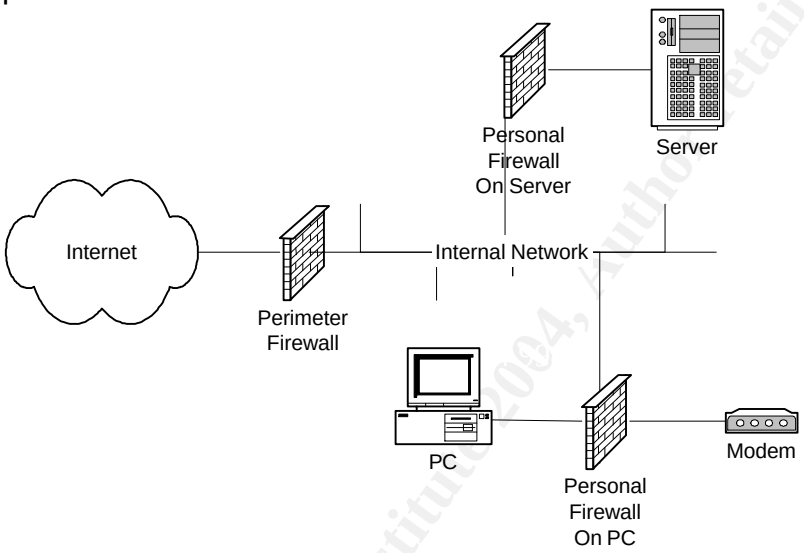
1. That your machine was trying to use ICMP or ping to count up through a network range.
2. That port 135 had traffic outbound from your machine (which was trying to exploit the DCOM RPC vulnerability)
3. That a connection was trying to be made on port 666 to 765 (707 was very common) incoming. The remote sat and waited to receive instructions on this port.

If personal firewall had been deployed on the desktop it would have been able to help contain the infections that had occurred. The non-infected machines would have been

able to defend themselves against the attack and slowed the spread of the worm. This worm was dangerous because it actually could bring a network to a crawl with all the network traffic that it created and in a very short period of time cripple your network. Even antivirus and firewall software will not protect you 100% if your system is unpatched with known security vulnerabilities.

The personal firewall in a small organization should be considered mandatory if your organization allows modems to be attached to PC's attached to the Local Area Network (LAN). Large organizations typically will ban modems use (or at least greatly restrict them) as they can create a great security hole that bypasses the corporate firewalls. In a small organization it may not be as understood as to why the modem is a security threat, the personal firewall could alert you to something that's not normal that is trying to connect to your system.

Below is an example of where firewalls should be deployed in a small charity. The perimeter firewall would be a hardware device like a DSL router.



A personal firewall on each machine can help round out the layered security and can end up being your last line of defense in the case of an attack. There are several good desktop firewalls that are available, popular firewalls are provided by: Zonelabs, Tiny Personal Firewall, Symantec's Norton Personal Firewall and Mcafee Personal Firewall Plus.

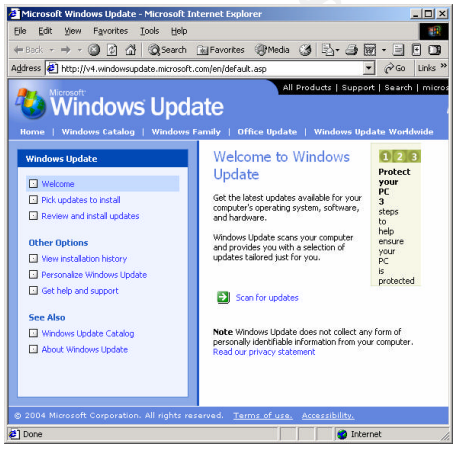
Patching

There are many ways to patch a system. Microsoft has multiple products to patch their systems. Windows Update (web), Software Update Services [SUS], System Management Server [SMS] are three Microsoft provided solutions. You can even decide to download these patches and hot fixes directly via FTP or HTTP. Of the three options only SMS requires purchase of a license. It should be noted that even though a patch is available it might not be available for each of the update options immediately. Microsoft states that for SUS updates can lag behind 2-3 hours after Windows Update has been updated although they strive to update at the same time (from the SUS FAQ http://www.microsoft.com/windowsserversystem/sus/susfaq.mspx). For a small organization the probably the preferred method is going to be Windows Update. Windows Update needs to be setup to run and download automatically.

The process for manually updating (forcing Windows update to run) is to open the Start menu as seen to the left This can be used to force a check to see if your machine is up to date.

Note about Software Update Services
If you have a number of machines or low bandwidth you can implement the Microsoft SUS system. Installing this is relatively complex. A great amount of time will be spent initially setting up a SUS server. The benefit is reduced bandwidth usage to download patches. For this paper I will limit discussion of SUS to making you aware it exists and provide links for additional reading. Please follow the URLs if you want to read about deploying SUS.
http://www.microsoft.com/sus/
http://www.susserver.com/

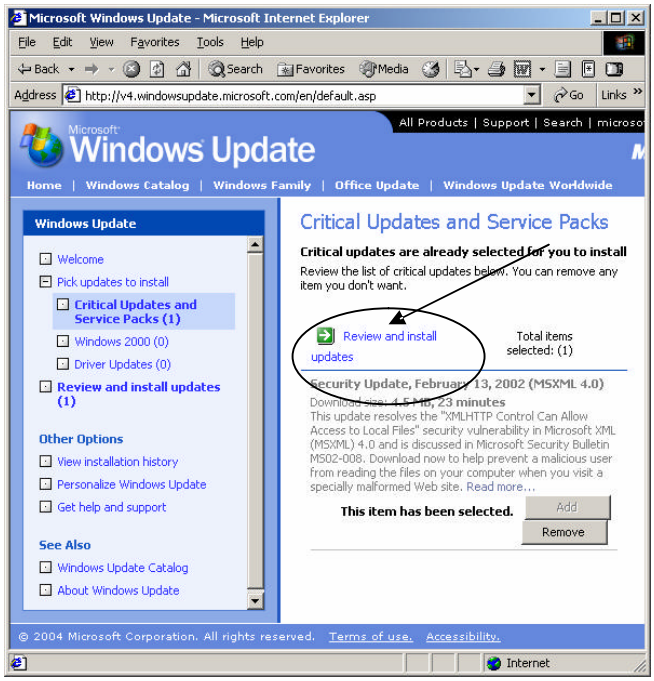
If you are interested in Microsoft security in general you can refer to http://www.microsoft.com/security/.

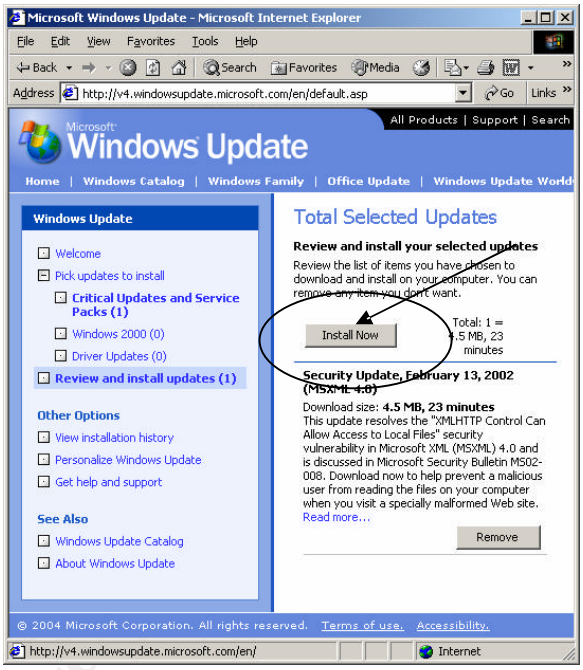


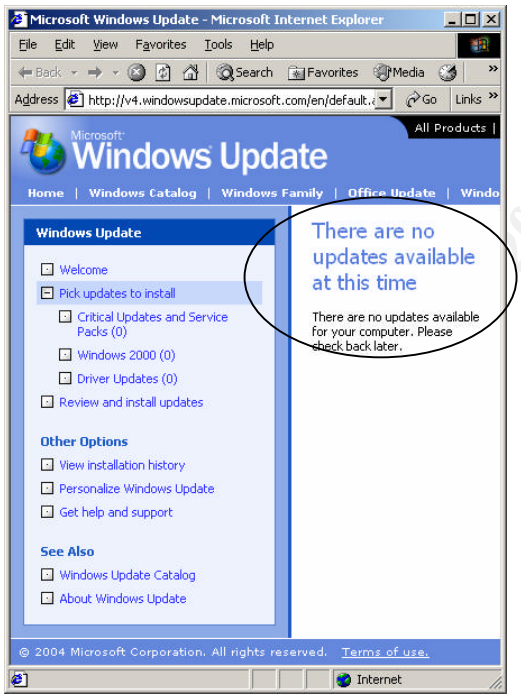
This will open the Windows Update website listed at http://v4.windowsupdate.microsoft.com/en/default.asp if you are running Microsoft Windows 2000 Professional.

At his point click scan for updates. The site will make sure your Windows update software is up to date.

Scanning may take a minute or two depending on your Internet connection speed. Once it has scanned it will give you a list of all the updates that are outstanding for your computer.

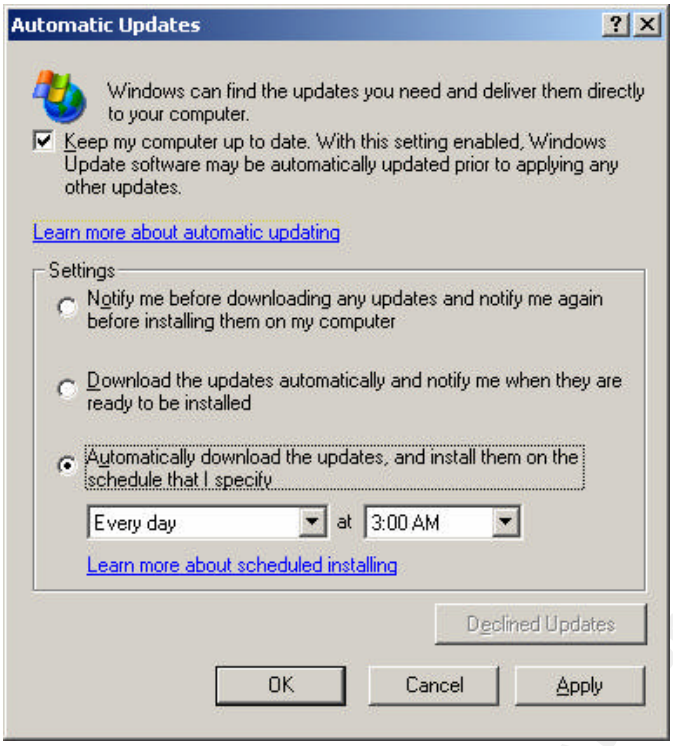






It should be noted that not all updates can be downloaded at the same time. Some updates will require that you reboot your system and rerun the Windows Update service. Windows update will also require that you patch the Critical Updates and Services packs before the general updates. This is to ensure that any security related patches are applied first to make sure that your system is not at risk for known vulnerabilities. Once you have completely patched your system you should see a screen similar to the following.

Continue running until you “There are no updates available at this time”.



Once you have patched your systems and have it up-to-date, the best option is to check for updates automatically and schedule them to be downloaded.

To set this up go to:
Start, Settings, Control Panel, Automatic Updates (Windows 2000)

It is important for the checkbox to be checked to enable the Windows Update.

Ideally the third radio button should be selected to force the download and install at the schedule specified.

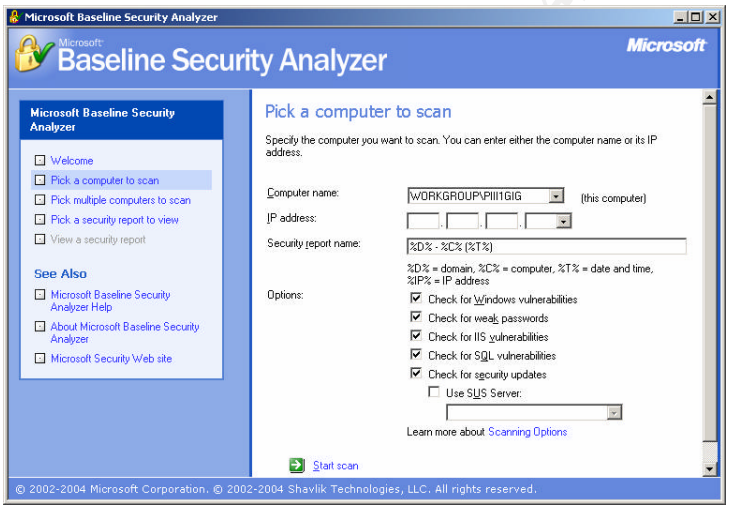
The time is important which you select. If the PC is turned off the schedule will not run. For a small company the optimal time may be just after everyone arrives (10:00AM). This will guarantee that the update will be run at the scheduled time.

Microsoft Baseline Security Analyzer

Once you have set your machines to be patched under a schedule you should download the Microsoft Baseline Security Analyzer. The current version at the time of writing is 1.2 and is available at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/mbsahome.asp
This is a utility that Microsoft has developed to check multiple Microsoft operating systems and Microsoft products.

This is the opening screen.

From here you can scan a single computer, multiple computers or view existing security reports.

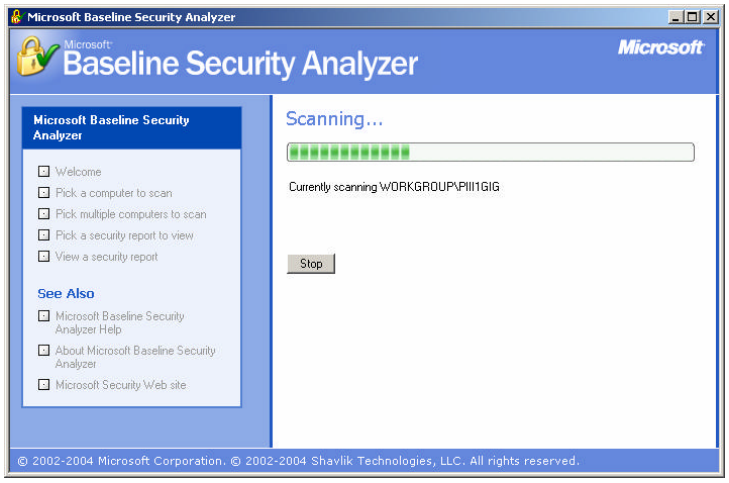


If you select Pick a computer to scan you will see the following screen.

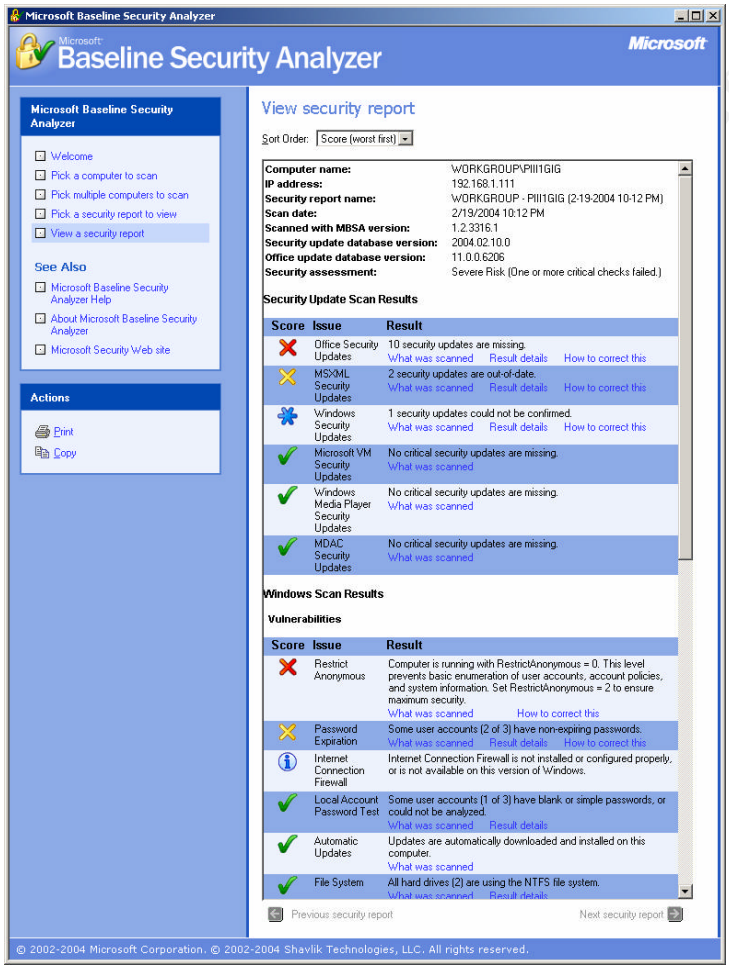
At this point you can select a by name or IP address.

Note how you can change the report names with the variables provided.

Click Start Scan



The scan will take a few minutes to complete.



This MSBA will allow you to see items relating to **Security Update Scan Results, Windows Scan Results, Additional System Information, Internet Information Services (IIS) Scan Results, SQL Server Scan Results and Desktop Application Scan Results.**

The MBSA utility gives a score, issue description and result. Within each category it also give “What was Scanned”, “Result Details” and “How to correct this.

This is utility gives you the opportunity to address the “known” vulnerabilities with your operating system and office products. It will pick out details that just running a Windows Update will not. This helps make you aware of items that a default operating system,

Microsoft SQL or Office install will setup insecure. You can explore the results by clicking on the blue text. The most interesting is to click on the "how to fix" and it will give you step-by-step instructions on how to fix the vulnerability.

A list of products from Microsoft's website that MSBA version 1.2 will scan for vulnerabilities:

> " MBSA runs on Windows 2000, Windows XP, and Windows Server 2003 systems and will scan for common system misconfigurations in the following products: Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003, Internet Information Server (IIS), SQL Server, Internet Explorer, and Office. MBSA 1.2 will also scan for missing security updates for the following products: Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003, IIS, SQL Server, IE, Exchange Server, Windows Media Player, Microsoft Data Access Components (MDAC), MSXML, Microsoft Virtual Machine, Commerce Server, Content Management Server, BizTalk Server, Host Integration Server, and Office."
>
> "Microsoft Baseline Security Analyzer V1.2"
> URL:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/mbsahome.asp (10 Feb 2004)

An example output from MSBA can be seen in Appendix B.

Policy

Any security initiative is backed by sound security policy and management support of the policy. It is important to write a security policies that minimally addresses the following:

- Strong passwords
  - Should be 8 characters or more
  - Should not be easy to guess (no children, spouse, pet's, sports team names)
  - Should not be shared, printed on a sticky note or otherwise wrote down
  - A good example of how to pick a secure password is to use the first letter of every word in a sentence or phrase changing case and letters to numbers.
    - **I want to go swimming on the weekend** could be translated to **1w2GsotW** which provides a stronger and harder to guess password but easy to remember.
  - If passwords need to be stored (for backup persons in the case you are absent) it is a good idea to use a password safe. A password safe is a secure database where the database is encrypted to ensure security of passwords.
    - The password database should be stored in a secure place on the network with only those who need access granted access.
    - You will need to write down one password (for the password safe), store it in an envelope with signatures and keep it in a safe place (company safe, managers locked filing cabinet etc.)
    - This way you still provide access to your accounts (this will put your manager at ease) but is not as easy to walk off with as an envelope filled with passwords. The password to the password safe is not the only piece of information required you will also be required to have access to the secure location on the network. Giving the passwords layers of protected security.
    - One freeware password safe with strong encryption can be found at http://www.schneier.com/passsafe.html
    - If you need a more robust password storage solution you can look at the solution by MAFIS Systems GbR. The Professional version stores all passwords in an encrypted database with integrated user and group rights administration. This will allow you to hide certain passwords completely (other than from an administrator of the database) or share them (for items like a print server that only allow one user id and password).
      - One interesting feature this software has is a log to let you know if your password has been accessed by someone within your group (legitimately of course). This gives traceability that using a piece of paper in an envelope doesn't. The software can be found at

http://www.passwordsafe.de/ and does require licensing beyond the demo period.

- Acceptable use of company resources
    - Do you want employee's using the Internet for person use? Personal gain?
    - A good Acceptable Use policy can help in a liable suit if you have had each employee sign that it is unacceptable to use company resources for non-business purposes and the policy has been consistently and fair in its application.
- Storage of passwords on local machines should be
    - Employees should be discouraged from letting Internet browsers store passwords for easy access.
        - This allows anyone who uses the machine to use these passwords and impersonate the other user.
        - It also allows hackers to gain access to accounts if a machine is compromised
- It is important to have all passwords from system administrators in case of illness etc.
- Not everyone should be a system administrator. Every administrator account increases the likelihood that a would be hacker will find an account that they can exploit.
- Limit the installation of non business applications
- Security awareness program

Writing the policy is just the first step. Second it must be approved and accepted by management before going any further in application.

Once accepted, it must be published and understood (hopefully signed off also) by each employee. Usually steps one and two are the easy ones. Step three is the hard one to enable. Ongoing communication and consistency is key to have a truly usable security policy.

For some excellent examples of policy templates view the SANS Institute at http://www.sans.org/resources/policies/#template. This can provide a start in creating your new security policies.

Disaster Planning

Disaster recovery relates to the availability of a system. Disaster recovery is all about anticipating the conceivable threats and planning for it. There is a saying in the disaster recovery industry “Fail to Plan; Plan to Fail”. (http://www.cmpnetasia.com/ViewArt.cfm?Artid=22011&Catid=4&subcat=43). Disaster recovery is all about planning and in essence is like an insurance policy. You hope you will never need it but you sure wouldn’t want to be without it when things go wrong. The Disaster Recovery Institute has an excellent Seven-Step Business Continuity Planning Model.
The seven steps are:

1. Project Initiation Phase
2. Functional Requirements Phase
3. Design and Development Phase
4. Implementation Phase
5. Testing and Exercising Phase
6. Maintenance and Updating Phase

   If Disaster Occurs
7. Execution Phase

(http://www.drii.org/associations/1311/files/planningmodel.pdf)

One thing to keep in mind is that it isn’t necessarily one thing that will create the crisis it is usually a combination of two or more things that go wrong. As an example a server hard disk could crash. Planning for disaster you would have found that:

- A single hard disk in a server if it failed would stop the server – purchasing a second hard disk and mirroring to it would allow one disk to fail and give you a window to replace the disk.
- Checking logs daily would have found that the drive was failing and given you the opportunity to replace the disk before it failed
- Doing periodic restores of data will ensure you are confident with a restore if needed and that the process is working – tape drives DO fail.

Disaster Planning can be as simple as the above example or as in depth as having a full hot server room located across the continent with individuals and equipment dedicated to the process. The initial cost for a small organization can be the time involved in the planning. Once you have done the planning the natural progression will be to mitigate the risks.

Free/Open Source Tools

There are several other tools that can be used to secure your Microsoft and non-Microsoft systems. There are several tools available and I am only going to mention a few. I recommend using up-to-date versions of all these software packages (including the Microsoft Baseline Security Analyzer. You can even use the Free/Open source tools to check that the MBSA caught everything! Freeware and Open source tools have come a long way over the past few years. The installation, interfaces and functionality of these products are rivaling software that you purchase for are available commercially for a fee.

NMap is an interesting tool for checking for open services on a system or device. It is easy to install and use. NMap can be found at www.insecure.org/nmap.

After running from NMap against a laptop on my network I found out that it was running several services that are undesirable (see table below).

1. It was running an HTTP server services but was not a “web server” (port 80, 443)
2. It was setup running the VNC server. If this is a service that is not needed (remote desktop sharing) then it should be disabled or patched per bulletin http://www.kb.cert.org/vuls/id/598581

As you can see the results are different when running a firewall and not running a firewall (see table below).

Without Zonealarm running	With Zonealarm running
Starting nmap V. 3.00 (www.insecure.org/nmap) Insufficient responses for TCP sequencing (3), OS detection may be less accurate Interesting ports on IS-LAPTOP (192.168.1.174): (The 1581 ports scanned but not shown below are in state: closed) Port State Service 7/tcp open echo 9/tcp open discard 13/tcp open daytime 17/tcp open qotd 19/tcp open chargen 42/tcp open nameserver 53/tcp open domain 80/tcp open http 135/tcp open loc-srv 139/tcp open netbios-ssn 443/tcp open https 445/tcp open microsoft-ds 1025/tcp open NFS-or-IIS 1026/tcp open LSA-or-nterm 1031/tcp open iad2 1032/tcp open iad3 3372/tcp open msdtc 3389/tcp open ms-term-serv 5800/tcp open vnc-http 5900/tcp open vnc Remote OS guesses: Windows NT 5 Beta2 or Beta3, Windows Millennium Edition (Me), Win 2000, or WinXP, MS Windows2000 Professional RC1/W2K Advance Server Beta3 Nmap run completed -- 1 IP address (1 host up) scanned in 9 seconds	Starting nmap V. 3.00 (www.insecure.org/nmap) Note: Host seems down. If it is really up, but blocking our ping probes, try -P0 Nmap run completed -- 1 IP address (0 hosts up) scanned in 30 seconds

SuperScan is another port scanner. It shows information in a little different format. It is available at http://www.foundstone.com/.

As you can see it brought back some different information with it. It queried the ports that were open and brought back information available on that port.

Sample SuperScan output

```
* + 192.168.1.174
        |___   7  Echo
        |___   9  Discard
        |___   13  Daytime
                |___ 7:04:03 PM 2/21/2004.
        |___   17  Quote of the Day
                |___ "My spelling is Wobbly.  It's good spelling but it Wobbles, and the letters.. get in the wrong places." A. A. Milne (1882-1958)
        |___   19  Character Generator
                |___  !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefg..!"#$%&'()*+,-
./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTU
        |___   42  WINS Host Name Server
        |___   53  Domain Name Server
        |___   80  World Wide Web HTTP
                |___ HTTP/1.1 404 Object Not Found..Server: Microsoft-IIS/5.0..Date: Sun, 22 Feb 2004 00:04:05 GMT..Content-Type: text/html..Content
        |___   135  DCE endpoint resolution
        |___   139  NETBIOS Session Service
        |___   443  https  MCom
        |___   445  Microsoft-DS
        |___   1025  network blackjack
        |___   1031  BBN IAD
        |___   1032  BBN IAD
        |___   5800  Virtual Network Computing server
        |___   5900  Virtual Network Computing server
                |___ RFB 003.006.
```

The use of these plus other free tools greatly enhances the security of the systems that you administrate. There are countless others that are available on the Internet through a search with your favorite search engine. One word of caution, I would suggest tools that others in the security community endorse. It is all too easy for someone to modify the tool for a malicious intent. I would also recommend downloading the tools directly from the author's web site and not mirrors for the same reason.

Summary

Basic security for a charity or small organization needs not be expensive or difficult to implement. The largest cost items were the antivirus software and firewalls, which bundled together from a commercial software company, will only cost $59.00 per machine. All the tools described for patching and scanning are available for free. The interfaces for these tools are easy enough that a person with basic Windows skills should be able to install and run. If you are willing to spend the time learning the output from the tools it will save in security consulting fees for the obvious threats. Through the proper application of Antivirus software, firewalls, system patching, sound security policy & communication, disaster planning and use of freely available tools you can secure your organization for a very reasonable price.

Appendix A

List of Products

All prices are approximate and are provided as an example of pricing only. If you wish to purchase please request a quote from your favorite reseller or check the web.

Antivirus Solutions

Charity and Non-profit organizations can get discounts on AVG Anti-Virus by Grisoft you will need to contact Grisoft directly to get a price.
http://www.grisoft.com/us/us_contact.php $33.00

http://www.symantecstore.com/dr/sat3/ec_MAIN.Entry17c?CID=48782&SID=27674&SP=10007&PN=5&PID=582926&DSP=&CUR=840&PGRP=0&CACHE_ID=48782 $49.00

http://us.mcafee.com/root/package.asp?pkgid=100 $34.95

Firewall Solutions

http://www.zonelabs.com/store/content/company/products/znalm/freeDownload.jsp
FREE

http://us.mcafee.com/root/package.asp?pkgid=103 $39.95
http://www.zonelabs.com/store/content/catalog/products/sku_list_zaplus.jsp?lid=pdb_plus $39.95

http://www.tinysoftware.com $49.00

http://us.mcafee.com/root/package.asp?pkgid=103 $39.99

Combined Antivirus/Firewall Solutions

http://www.symantecstore.com/dr/sat3/ec_MAIN.Entry17c?CID=48782&SID=27674&SP=10007&PN=5&PID=584414&DSP=&CUR=840&PGRP=0&CACHE_ID=48782 $69.00

http://us.mcafee.com/default.asp $59.00

Password Managers

http://www.schneier.com/passsafe.html FREE

http://www.symantecstore.com/dr/sat3/ec_MAIN.Entry17c?CID=48782&SID=27674&SP=10007&PN=5&PID=584422&DSP=&CUR=840&PGRP=0&CACHE_ID=48782 $39.00

http://www.passwordsafe.de/ depending on the number of licenses purchased and version $33.00 per license

Appendix B

MSBA – Microsoft Baseline Analyzer Output

Computer name:	WORKGROUP\PIII1GIG
IP address:	192.168.1.111
Security report name:	WORKGROUP - PIII1GIG (2-19-2004 10-12 PM)
Scan date:	2/19/2004 10:12 PM
Security update database version:	2004.02.10.0
Office update database version:	11.0.0.6206
Security assessment:	Severe Risk (One or more critical checks failed.)

Security Updates

Score	Issue	Result
Check failed (critical)	Office Security Updates	10 security updates are missing. **Update** Access 2000 Snapshot Viewer Security Patch: KB826292 (English version) This update requires Office 2000 Service Pack 3 (English version) to be installed first. Excel 2000 Security Patch: KB830349 This update requires Office 2000 Service Pack 3 (English version) to be installed first. Office 2000 Security Patch: KB822035 This update requires Office 2000 Service Pack 3 (English version) to be installed first. Office 2000 Service Pack 3 (English version) This update requires Office 2000 Service Release 1a (English version) to be installed first. Office 2000 Service Release 1a (English version) Office 2000 WordPerfect 5.x Converter Security Patch: KB824993 (English version) This update requires Office 2000 Service Pack 3 (English version) to be installed first. Outlook 2000 Collaboration Data Objects (CDO) Update: Security (English version) This update requires Office 2000 Service Pack 3 (English version) to be installed first. Outlook 2000 Update: December 18, 2002 (English version) This update requires Office 2000 Service Pack 3 (English version) to be installed first. Visio 2002 Security Patch: KB822212 Word 2000 Security Patch: KB830347 This update requires Office 2000 Service Pack 3 (English version) to be installed first.
Check failed (non-critical)	MSXML Security Updates	2 security updates are out-of-date. **Security Update** / **Description** / **Reason** MSXML 3.0 / MSXML 3.0 SP3 / The latest service pack for this product is not installed. Currently SP3 is installed. The latest service pack is SP4. MSXML 4.0 / MSXML 4.0 SP1 / The latest service pack for this product is not installed. Currently SP1 is installed. The latest service pack is SP2.
Best practice	Windows Security Updates	1 security updates could not be confirmed. **Security Update** / **Description** / **Reason** MS03-030 / Unchecked Buffer in DirectX Could Enable System Compromise (819696) / Please refer to 306460 for a detailed explanation.
Check passed	Microsoft VM Security Updates	No critical security updates are missing.
Check passed	Windows Media Player Security Updates	No critical security updates are missing.
Check passed	MDAC Security Updates	No critical security updates are missing.

Windows Scan Results

Vulnerabilities

Score	Issue	Result
Check failed (critical)	Restrict Anonymous	Computer is running with RestrictAnonymous = 0. This level prevents basic enumeration of user accounts, account policies, and system information. Set RestrictAnonymous = 2 to ensure maximum security.
Check failed (non-critical)	Password Expiration	Some user accounts (2 of 3) have non-expiring passwords. **User** Administrator Guest

		ASPNET
Best practice	Internet Connection Firewall	Internet Connection Firewall is not installed or configured properly, or is not available on this version of Windows.
Check passed	Local Account Password Test	Some user accounts (1 of 3) have blank or simple passwords, or could not be analyzed.

User	Weak Password	Locked Out	Disabled
Guest	Weak	-	Disabled
ASPNET	-	-	-
Administrator	-	-	-

Check passed	Automatic Updates	Updates are automatically downloaded and installed on this computer.
Check passed	File System	All hard drives (2) are using the NTFS file system.

Drive Letter	File System
C:	NTFS
D:	NTFS

Check passed	Autologon	Autologon is not configured on this computer.
Check passed	Guest Account	The Guest account is disabled on this computer.
Check passed	Administrators	No more than 2 Administrators were found on this computer.

User
Administrator

Additional System Information

Score	Issue	Result
Best practice	Auditing	Enable auditing for specific events like logon/logoff. Be sure to monitor your event log to watch for unauthorized access.
Best practice	Services	Some potentially unnecessary services are installed.

Service	State
Telnet	Stopped

Additional information	Shares	3 share(s) are present on your computer.

Share	Directory	Share ACL	Directory ACL
ADMIN$	C:\WINNT	Admin Share	BUILTIN\Users - RX, BUILTIN\Power Users - RWXD, BUILTIN\Administrators - F, NT AUTHORITY\SYSTEM - F, Everyone - RX
C$	C:\	Admin Share	Everyone - F
D$	D:\	Admin Share	Everyone - F

Additional information	Windows Version	Computer is running Windows 2000 or greater.

Internet Information Services (IIS) Scan Results

Score	Issue	Result
Check not performed	IIS Status	IIS is not running on this computer.

SQL Server Scan Results

Score	Issue	Result
Check not performed	SQL Server/MSDE Status	SQL Server and/or MSDE is not installed on this computer.

Desktop Application Scan Results

Vulnerabilities

Score	Issue	Result
Check failed (critical)	IE Zones	Internet Explorer zones do not have secure settings for some users.

User	Zone	Level	Recommended Level
PIII1GIG\Administrator	Restricted sites	Custom	High

Setting	Current	Recommended
Script ActiveX controls marked safe for scripting	Enable	Disable

Check failed (non-critical)	Macro Security	4 Microsoft Office product(s) are installed. Some issues were found.

Issue	User	Advice
Microsoft Outlook 2000	PIII1GIG\Administrator	Macro security is set to medium, which will allow you to choose whether or not to run potentially unsafe macros.
Microsoft PowerPoint 2000	PIII1GIG\Administrator	Macro security is set to medium, which will allow you to choose whether or not to run potentially unsafe macros.
Microsoft Excel 2000	All Users	No security issues were found.
Microsoft Word 2000	All Users	No security issues were found.

Appendix C

Glossary

NAT – Network Address Translation

The use of network address translation is pretty well a standard in the Internet community now. What is allows is for multiple machines/devices (possibly hundreds or thousands) to be represented by a single IP address to the other side of the “NATing” device (usually the Internet). Network address translation part of the short term solution to the shortage of IP addresses globally.

Stateful Inspection – is also referred to as dynamic packet filtering. The firewall not only looks at the header information but also looks at the contents of the packet and monitors the state of the connection.

Appendix D

References

Internet Sources (URLs):

"Windows 2000 Service Pack 4 Network Install for IT Professionals." 26 June 2003. URL:http://www.microsoft.com/downloads/details.aspx?FamilyID=1001aaf1-749f-49f4-8010-297bd6ca33a0&DisplayLang=en (2 Feb 2004)

"Symantec Security Response - Search and Latest Virus Threats Page." 20 Feb 2004. URL:http://securityresponse.symantec.com/avcenter/vinfodb.html (22 Feb 2004)

"Zone Labs Zone Labs Press Releases." 15 Dec 2003 http://www.zonelabs.com/store/content/company/aboutUs/pressroom/pressReleases/2003/pr_50.jsp (15 Feb 2004)

Nahorney, Benjamin and Douglas Knowles, Frederic Perriot. "Symantec Security Response - W32.Welchia.Worm." 16 Dec 2003. URL:http://securityresponse.symantec.com/avcenter/venc/data/w32.welchia.worm.html (2 Feb 2004)

18 Aug 2003. URL:http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=100559 (20 Feb 2004)

"Microsoft Baseline Security Analyzer V1.2" URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/mbsahome.asp (10 Feb 2004)

Heng, Dr Goh Moh. "Fail to Plan; Plan to Fail" 1 Nov 2003. URL:http://www.cmpnetasia.com/ViewArt.cfm?Artid=22011&Catid=4&subcat=43 (16 Feb 2004)

URL: http://www.webopedia.com/TERM/S/stateful_inspection.html (16 Feb 2004)

URL: http://www.drii.org/associations/1311/files/planningmodel.pdf (18 Feb 2004)