



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at <http://www.giac.org/registration/gsec>

Scaling Enterprise Security to the SOHO:
A Fundamental Approach to Affordable Security

By
Don Berlin
December 20, 2003

GIAC Security Essentials Certification
Practical Assignment
Version 1.4b

© SANS Institute 2004, Author retains full rights.

Table of Contents

<u>Table of Figures</u>	iii
<u>Abstract</u>	iv
<u>Introduction</u>	1
<u>The Enterprise Security Model</u>	2
Defense in-Depth	2
<u>Firewalls</u>	3
Overview	3
Hardware-based	4
Software-based	4
Recommendation	5
A Deeper Look	6
Moving On	9
<u>Anti-Virus</u>	9
Overview	9
E-mail	9
Worms	10
Web Pages	10
Recommendation	10
A Deeper Look	11
<u>Patch Management</u>	13
Overview	13
Windows Update	13
Software Update Services (SUS)	14
Recommendation	14
A Deeper Look	15
<u>Operating System Hardening</u>	19
Overview	19
Microsoft Baseline Security Analyzer	19
Security Configuration Manager	21
Recommendation	22
A Deeper Look	23
<u>User Awareness</u>	24
<u>Conclusion</u>	27
<u>Appendix A - Description of Malware Terminology</u>	29
<u>Appendix B – Secure Workstation Template</u>	31
<u>Works Cited</u>	36

Table of Figures

Table 1: Recommended Firewalls	6
Table 2: Network Address Translation	7
Table 3: User Awareness Topics	26

© SANS Institute 2004, Author retains full rights.

Abstract

The purpose of this document is to scale the Enterprise security model to that of the Small Office/Home Office (SOHO) Windows environment. In doing so, this document scales the discourse from the corporate expert to the neophyte SOHO reader. However, it is anticipated that some readers will be experts (sysadmin, netadmin, etc), in their own right, yet, are not as knowledgeable about security as they may desire to be. Thus, each topic includes an in-depth technical discussion intended for the expert to complement the more general discussion presented to the novice. The dialogue begins with a brief summary of the Enterprise security model and then carries on to present a perimeter-to-core approach to developing a complete information security solution.

The author presumes that the reader agrees that effective, comprehensive information security is necessary and has sought out this document to assist in creating such an environment. Therefore, the author does not besiege the reader with fantastic statistics or melodrama. The paper takes a fundamentals approach to securing the SOHO domain in a manner consistent with that of large corporations.

The topics reviewed include hardware- and software-based firewalls, anti-virus protection, operating system (OS) patching, OS hardening, and user awareness. The novice PC user can use the document as a checklist to securing the SOHO environment with the opportunity to return to the document at a later time to gain a deeper knowledge of each defense layer; while the sys/net-admin can use the document to gain further understanding of the concepts involved with securing the SOHO environment all the while implementing each.

Introduction

Over the past several years, information security has really come to garner the attention that it requires. Corporations have finally begun to take information security seriously and have altered their budgets to appropriate monies to bring their enterprise security into compliance with the expectations and recommendations of security experts. With the arrival of affordable broadband Internet service, and the corporate focus on Internet security, small businesses and home users are now beginning to bear the burden of the crackers and script kiddies. Of course, the big corporations are still prime targets, but with their improved security, the bad-guys are enlisting (involuntarily, I might add) the aid of the small businesses and home users. Moreover, the threat to the SOHO user is more than being a pawn in a distributed denial of service (DDoS) attack on corporations; the user is also in danger of having their private personal information (i.e. social security or credit card numbers) compromised, their computers damaged, or becoming the unwitting purveyor of hacker warez and pornography.

We all, corporations; small-businesses; and individuals alike, share the responsibility to do our part to help secure cyberspace. However, as you are probably thinking as you read such an assertion, we do not all have the requisite knowledge, expertise, or funding of a large corporation. Not to worry, as we progress through this paper, it will become clear that the security model that the large corporations use to protect their information can be scaled to fit a SOHO Windows* environment that is well within most any budget constraint. The dialogue will be presented in such a manner that the novice user can use the paper as a checklist to securing their environment, while the knowledgeable (system administrator, et. al.) user can expand her knowledge of each topic all the while implementing it.

We will begin with a synopsis look at the enterprise security model where we will see that, aside from the knowledgeable staff and funding, there is scarce difference between the needs and structure of the SOHO environment and that of the corporate environment. Within this overview, we will establish the individual topics that are in common between the two environments and set up for the examination of each in detail. Each section will include an overview of the topic, a description of the tools available (if applicable), a recommended course of action, and an optional, in-depth, technical look into the topic.

* "...shipments of Microsoft's server operating systems grew from 50.5 percent of the market in 2001 to 55.1 percent last year, while shipments of its client operating systems increased from 93.2 percent to 93.8 percent worldwide."

Dyck, T. (2001).

The Enterprise Security Model

Defense in-Depth

Pragmatically speaking, no defense can be considered a perfect defense. The adage, “if there is a will, there is a way” is quite applicable to our discussion. The circumstances of maintaining an “always on”[†] Internet presence are such that it is not a matter of *if* we will be hacked, but *when*. Large corporations are aware of this condition, and design their enterprise security posture accordingly. At the corporate level, a risk management team identifies which company resources would cause the company the greatest amount of harm if compromised, and therefore need safeguarding. It is around these resources that the enterprise security model is developed.

The effective enterprise security model has many protective measures in place. The phrase commonly used when referring to these protections is “Defense in-Depth”. The theory behind the defense in-depth model is such that if one safeguard was to fail, another safeguard is in place to protect our systems and data. To illustrate, a local organization has the following physical security design:

- All entrances to the facility are locked
- To gain entry to the facility, one must explain one’s purpose for visiting and with whom one is to visit
- Upon verification of said appointment, access is granted through the first door and logged
- Upon entering the first door of the facility, one must pass through a metal-detector
- After successfully passing through the metal-detector, access is granted through a second door
- Visitors are then escorted directly to the main office
- Once in the main office, credentials are presented verifying that one is indeed who one claims to be
- If the purpose of the visit requires access to any other area of the facility beyond the main office, a visitor badge is issued and an escort provided
- The entire facility is monitored by video cameras and each door that opens is recorded

The enterprise defense in-depth cyber security model emulates this layered approach to facility security.

- A router controls access to our network perimeter [locked door]. As traffic must meet the conditions specified on the router, it is here that we can initially accept or silently drop Internet traffic destined for our network.

[†]“Broadband services are referred to as “always-on” services because there is no call setup when your computer has something to send. The computer is always on the network, ready to send or receive data through its network interface card (NIC). Since the connection is always up, your computer’s IP address will change less frequently (if at all), thus making it more of a fixed target for attack.” CERT (2001). Home Network Security, Carnegie Mellon University.

-
- Subsequent to successfully meeting the conditions of the router's access control list [verification of appointment], the forwarded traffic encounters both the Network Intrusion Detection System (NIDS) and our firewall [metal detector].
 - On our NIDS, triggered alerts are logged and alert messages dispatched to a security operator.
 - Our firewall inspects the traffic, and upon satisfying the rules of the firewall, forwards the traffic to the intended destination [main office].
 - Upon reaching the intended destination, both the software-based endpoint firewall and the anti-virus software further scrutinize the traffic. A great deal of activity is taking place at this moment. The endpoint firewall may block the traffic, or the anti-virus software may stop the traffic payload.
 - If the purpose of the traffic is to engage a particular service, then the service prompts for authentication [present credentials].
 - A successful logon to the service grants the sender of the network traffic access to the provided service [visitor badge and escort].
 - The server's Host Intrusion Detection System (HIDS) logs the connection to the service, and any associated file access [monitor & record].

Clearly, we can see the multiple defensive layers and can begin to appreciate the value of such a strategy. If knowledge and funding were not an issue, I would certainly recommend that the SOHO user implement the security model just described. However, if knowledge and money were not an issue, you would not be reading this document.

As I mentioned in the introduction, this document will scale the enterprise security model to meet the security needs of the SOHO setting. Consequently, we do not require quite as many layers in our defense tactic. I have chosen what I believe to be the five defensive layers that no environment of any size can do without. Each of these layers is equally important, thus I do not discuss them in order of importance, but in order of outside-in, perimeter to core.

The perimeter of our SOHO environment will need the protection of a firewall.

Firewalls

Overview

Before we discuss why firewalls are necessary, and go on to suggest which firewalls may be best suited for our SOHO environment, I expect that it would be sensible to provide a sentence or two explaining what a firewall is. In the brick-and-mortar world, a firewall provides a protective barrier between two objects. For example, a firewall separates the individual dwellings in a senior citizens apartment building; thus, inhibiting a small fire in one dwelling from quickly spreading to the next. In the virtual world, the premise is quite the same as we desire to separate our internal network systems and data from undesirable Internet traffic.

Marcus J. Ranum and Matt Curtin offer the following definition of a firewall in the firewall section of the faqs.org website:

"A firewall is a system or group of systems that enforces an access control policy between two networks. The actual means by which this is accomplished varies widely, but in principle, the firewall can be thought of as a pair of mechanisms: one exists to block traffic, and the other exists to permit traffic." ‡

While this certainly is an accurate high-level description of a firewall, it is a little too general to help you to form a good mental picture of what a firewall is. Therefore, I prefer to share with you another simple analogy that I use when discussing the necessity of perimeter security with my users:

A firewall is essentially an electronic version of a traffic officer. Just as a police officer, trained in traffic law and assigned to traffic-control detail, redirects, or stops, automobile traffic, a firewall configured with the network traffic rules that are specific to our individual business requirements, redirects, or drops, the Internet traffic destined for our network.

At one time, firewalls were commonly thought of as hardware devices, however just as our security model has evolved, so have firewalls. Today, we find two forms of firewalls: hardware-based and software-based.

Hardware-based

Small-office/home-office hardware-based firewalls are small self-contained physical devices that contain some type of hardened operating system and configuration software. The devices typically offer the capacity to directly connect from 5 to 16 servers or PCs, thus one device can protect the entire SOHO perimeter. The configuration software provided has improved dramatically just in the last eighteen months. The hardware firewalls now feature a quite secure *default* configuration that literally permits the novice user to plug the device in, follow a wizard-style configuration procedure and essentially "set it and forget it". These devices offer NAT, DHCP, SPI, IP and MAC filtering, DMZ, URL blocking, Usage Schedules, IDS, VPN, DDNS, UPnP, and logging. Do not worry about the alphabet soup; we will discuss most of these in *A Deeper Look*. For now, just trust me that these services, and granular control, are a good thing once you have become more experienced at firewall security.

Software-based

In contrast to the hardware device, software-based firewalls require you to provide a host operating system, as well as the host hardware. The software firewall requires that you license (unless free version) and install it on each of the computers that you desire to protect. Software firewalls operate at the application level granting and preventing access to the network on an application-by-application basis. The default configuration of the newer software firewalls is secure, and most have been modified to include a common set of applications that are granted trusted access to the network, thus facilitating configuration for the novice user. Additionally, a user can

‡ Curtin, C. M. (2003). Firewalls FAQ.

create trusted, un-trusted, and blocked zones to assist network access control management. What is more, as a direct result of installation on each PC, the software firewall has intimate knowledge of the activity that takes place on the individual computer, a detail that is lost with the hardware based firewall device. Finally, if the payload of legitimate network traffic (e.g. a malicious email attachment) has compromised one of the PCs on your network, the software-based firewall will stop that infected PC from compromising the rest of the network. In this way, the software-based firewall acts just as the example given of a firewall in the brick-and-mortar world.

Recommendation

A great many hardware- and software-based firewall solutions exist on the market today. Both hardware and software forms of firewalls have evolved such that, in and of them, neither is better than the other is. To determine which form is right for your environment, you should answer the following questions:

1. How many PCs do you need to protect?
2. What kind of control are you looking for?
3. How much firewall knowledge does the person that will maintain the firewalls possess?

Only after having answered these questions, can you make the best decision for your situation. The following are general guidelines:

- If you must protect greater than four PCs, then you should strongly consider the hardware-based firewall device. Maintaining consistent software based policies across more than four PCs can be quite time consuming and tends to be error prone. Moreover, as upgrades become available, you can upgrade one hardware device and provide upgraded protection to all the PCs rather than having to upgrade each individual computer.
- If you desire application level control, or wish to prevent access to specific files and folders on the PC file system, you should consider the software-based firewall. Several versions of these firewall products allow you to configure access control to specific areas of the file system that is not available with the hardware device.
- If the person charged with maintaining the firewalls has moderate to strong networking skill, the hardware device offers excellent tools for creating a very secure networked environment beyond the already secure default configuration. If the person maintaining the firewalls is not so strong in the networking capacity, then the software-based solution may be the better solution providing control via application access.

Keep in mind, the software-based firewall protects the individual PC; whereas, the hardware-based device protects the entire internal network. Consequently, depending on how much budget you can allocate for this particular defensive layer, I would strongly recommend that you deploy both versions of the firewalls. Each form has features that the other does not. Thus, you can utilize the

strengths of each, compensate for the weakness of each, and all the while provide an extra layer of defense. And, after all, this discussion *is* about providing a layered defense!

To this point, I have used several hardware and software firewalls when setting up SOHO environments. I prefer the features of, and have had the best experience with, the list of firewalls in Table 1:

Software: ZoneLab's ZoneAlarm (www.zonelabs.com) Tiny Software's Tiny Personal Firewall (www.tinysoftware.com)
Hardware: SMC's Barricade (www.smc.com) Netgear's Prosafe (www.netgear.com)

Table 1: Recommended Firewalls

A Deeper Look

Although I offer my recommendations on each topic, I feel that it is important that you have a better understanding of the features of the concepts and tools mentioned. To this end, I will include a section (when applicable) covering the features in detail.

In the description of the hardware-based firewall device, I included quite a list of acronyms representing features of firewalls. Now, we will take a closer look at some of these features.

NAT (Network Address Translation)

While I certainly have not reviewed every router/firewall device, I feel comfortable stating that every commercially available router/firewall device offers NAT.

By using reserved, special use[§], IP-addresses internally, network address translation provides the ability to “shield” our internal network from the Internet. On the wide area network (WAN) port, the device uses the public IP-address assigned (dynamically or statically) by our internet service provider (ISP). On the internal port, the device uses a special use address. Internally, the device keeps track of which internal address made an Internet connection request, and to which web-server. The NAT service sends the request packet with the source address of the WAN port to the target web-server, and then translates the web-server response packet's destination address back to our special use address, thereby preventing any direct connection to our internal machines.

Table 2 demonstrates how the packet header would appear at each stage of the session:

[§] Y. Rekhter, B. M., D. Karrenberg, G. J. de Groot, E. Lear (1996). Network Working Group Request for Comments 1918.

If your spouse uses a laptop at 192.168.2.22 to open a web browser to make a connection to the local online newspaper's web server at 61.172.190.161, the computer creates an IP packet with the following data in it:

- Source IP address: 192.168.2.22
- Source port: 4090
- Destination IP address: 61.172.190.161
- Destination port: 80

The computer then forwards the packet to the NAT service on our firewall at 24.64.140.123 (WAN side). The NAT service translates our packet information to:

- Source IP address: 24.64.140.123
- Source port: 1028
- Destination IP address: 61.172.190.161
- Destination port: 80

Internally, the NAT service maintains a table that has our private address of 192.168.2.22:4090 mapped to our firewall WAN address of 24.64.140.123:1028. The firewall then forwards the packet over the Internet to the newspaper's web server. The web server sends a response packet back to our firewall that looks like this:

- Source IP address: 61.172.190.161
- Source port: 80
- Destination IP address: 24.64.140.123
- Destination port: 1028

Our NAT service looks up the destination address in its translation table and rewrites the packet addresses as mapped and forwards the packet on to your spouse's laptop. The packet data looks like:

- Source IP address: 61.172.190.161
- Source port: 80
- Destination IP address: 192.168.2.22
- Destination port: 4090

This process is repeated for every subsequent packet transmitted during this session with the web server.

Table 2: Network Address Translation

DHCP (Dynamic Host Configuration Protocol)

Dhcp.org offers this for the definition of DHCP: "... (DHCP) is an Internet protocol for automating the configuration of computers that use TCP/IP. DHCP can be used to automatically assign IP addresses, to deliver TCP/IP stack configuration parameters such as the subnet mask and default router, and to provide other configuration information such as the addresses for printer, time and news servers."** In our situation, DHCP allows us to simply plug in (to the network) each additional computer that we need and have the special use addresses automatically assigned and configured. The DHCP service runs on the router/firewall, and as long as our NICs are configured to use DHCP, all will be taken care of behind the scenes.

SPI (Stateful Packet Inspection)

Our default and user-configured rule sets typically only investigate the packet header when determining whether to accept or reject network traffic. Stateful packet inspection peers a little deeper into a packet than just the IP headers to determine how to deal with the traffic. The SPI process will attempt to

**Droms, R. (2003). Resources for DHCP.

determine whether a specific packet is part of an already-established session initiated from the internal network, or instead, a new session being initiated from the outside. Of course, depending on which criterion is fitting, the packet is passed or dropped. This “session” based approach allows us to provide fairly unrestricted outbound access for our users on the inside, while providing flexible, selective access from the outside.

IP (Internet Protocol)/MAC (Media Access Code) Filtering

The IP address is the specific address configured for our network interface card (NIC). This address is analogous to our residential address. Our residential address lets the postal worker find us to deliver our post; the IP-address lets network traffic find us to set-up and use network resources. The MAC address is a six-byte hexadecimal hardware address that uniquely identifies our NIC card. The IP address looks like 192.168.1.100, whereas the MAC address looks like 00-a0-c9-49-97-7d. We can configure our firewalls to restrict access to our network to only the IP or MAC addresses that we list as acceptable sources. Anytime a computer is connected to the network, this table is consulted to determine whether access can be granted to the associated IP or MAC address. If neither of the addresses is on the list, then access to the network is denied.

DMZ (Demilitarized Zone)

The following description of a DMZ can be found at InformIT.com, “Technically, a DMZ is its own little network, separate from the internal network, and separate from the Internet. This allows any Internet user to access the allocated resources on the server, but if the server becomes compromised, an attacker won't be able to use the "owned" computer to search out the rest of the network.”^{††} Furthermore, the rule set written to control access to the DMZ will be extremely restrictive, usually only allowing a specific protocol through to a server. For example, we would place a web server in the DMZ and our firewall rule would allow only HTTP and HTTPS to the web server, all other traffic to that web server address would be dropped. This type of restrictive access prevents inappropriate traffic from reaching our server. Any attempt to FTP or Telnet to the server would be stopped at the perimeter.

IDS (Intrusion Detection System)

An Intrusion Detection System works hand in hand with the SPI component to provide feedback via logging, reporting, and alert messages to the firewall administrator. Moreover, this service affords us the ability to drop traffic that matches certain patterns; patterns that could be Denial of Service (DoS) attempts.

^{††} Cyrus Peikari, S. F. (2003). Demilitarized Zone, Pearson Education, Inc.

VPN (Virtual Private Network)

The VPN component of our firewall allows us to create a private tunnel between a computer on our network and, say, a specific computer at our corporate headquarters. Using special protocols, a secure, encrypted session can be created between these two locations. Look to <http://www.iec.org/online/tutorials/vpn/> for an excellent online tutorial on VPNs.

Now that we have reviewed the recommended firewall features, I hope you can appreciate the significance of each. These essential features listed above grant us additional flexibility and control, thereby allowing us to create a more secure perimeter to our SOHO location. Entire book chapters have been written about these features, please follow the links provided, or search keywords on Google.com to further your education and more confidently secure your network perimeter.

Moving On

We have a hardware firewall separating our internal network/systems from the Internet, and we have reinforced that with a software firewall on each endpoint. We have read all of the product documentation, searched the Internet, and are confident that we have our firewalls configured properly; finally, we are secure! Right? Not yet! Although we have established a perimeter security posture capable of protecting us from a great many Internet borne attack vectors, we must move in one level and begin developing our next layer of defense.

Equally important and equally essential to our security model is anti-virus protection.

Anti-Virus

Overview

We have configured our perimeter security devices to prevent any non-approved access to our systems, but how secure is the approved access? During the normal course of business, our users may require/desire access to browse the Internet. Moreover, email is such an integral component to communication, as we know it, that we must grant access to our network for the email service. Thus, we have written our firewall rules to allow our internal users to establish http sessions on the Internet; and, we have written our firewall rules to permit e-mail transport. Is it coincidence then, that the most prevalent virus/malware threat vectors are e-mail attachments, e-mail messages, worms and web pages?

E-mail

Threats used to be simple and low-tech; e-mail messages contained embedded code, or cleverly disguised attachments. An attacker was effective if she could write a convincing email message that tricked the user into executing the e-mail attachment, or visiting the web page, that contained the

virus payload. The virus code was simple, straightforward and on the odd occasion non-malicious.

Worms

The simple, low-tech method evolved and the worm threat vector emerged. Attackers developed worms to avoid the need for human interaction and took advantage of system/application vulnerabilities. Worms do not spread via infection; worms spread via network shares, mass emailing (often with their own built in email engine), and from compromised machines scanning the Internet for their next victim.

The worm payload need not be viral. Commonly, the payload of choice is Trojan horses or spyware

Web Pages

The web page threat vector exploits the fact that web pages need only to be visited to initiate the malware/virus. A user need not click on any page content; simply browsing to the web page would allow the Java; JavaScript or ActiveX control to automatically execute. The executed malware/virus could potentially access files on the local system, or even install Trojans/spyware.

As clever and advanced as the second generation threat vectors are, the low-tech e-mail attachment is still the primary method of propagation. In fact, more computers are attacked when users carelessly open email attachments than by all other vectors combined^{‡‡} often resulting in expensive remediation.

Britain's Corporate IT Forum, an organization of IT professionals from some of the UK's largest blue-chip companies, estimates that each malware/virus incident costs an average of \$213,000 in man-hours and related costs^{§§}.

Recommendation

Antivirus software has evolved in-step with the viruses and malware and numerous companies offer antivirus products. When choosing your antivirus solution, take care to choose a product that:

- Frequently updates signature files
- Provides automatic updating of said signature files
- Provides on-access scanning
- Provides on-demand scanning
- Allows you to schedule automatic scanning tasks
- Integrates tightly with your e-mail application
- Offers advanced scanning techniques (boot-time, heuristics, archive files)
- Provides configuration locking

^{‡‡} Club, H. T. C. (2003). Attack Vectors.

^{§§} Mimoso, M. S. (2003). Cost of virus cleanups goes up, TechTarget.

Each of these features affords us the ability to more securely control the email threat vector. The majority of antivirus products come with the features that are listed; however, not all of them do so.

If you do not adjust any other user configurable setting, it is imperative that you set the product to automatically update. The manufacturer will recommend that you update at least weekly; I recommend that you schedule your antivirus product to update *daily*. Antivirus signature files that are even a day old can leave your system vulnerable to the latest virus.

While I prefer the McAfee VirusScan line of software, Symantec offers a fine product, too. You can find a list of the 15 most prevalent antivirus solutions at www.cert.org/computer_viruses/viruses.html.

Best Practices: suggest that you do not open any email attachments that you are not expecting. Even if the email purports to be from your mother, call her first and ask her if she sent you an email with an attachment. Do not just assume that the email attachment is safe because it appears to have come from Mom...

A Deeper Look

Frequently Updated Signature Files

Nearly everyday someone discovers a new virus, if you happen to be the unwitting discoverer; there is not much a signature based antivirus product can do for you. However, if you are not on the front line of the new virus, then you hope that your product vendor can get an updated signature file created quickly. The signature file contains patterns of code for known viruses. The antivirus (A/V) scanning engine compares the files on your hard disk, or in memory, to the signature file patterns to determine whether a file is infected.

While reactive by definition, updated signature files can be proactive for the majority of users. The typical vendor will release updated signature files on a weekly basis with an accelerated release rate for high concern viruses. Typically viruses are rated as to how quickly they spread and how much damage they inflict. McAfee provides an email notification service that informs you when a signature file is released for a virus rated medium or above.

Provides automatic updating of signature files

It is worth mentioning again that the most important user configuration you make to your A/V product is to set it up to automatically check daily for updated signature files. A/V signature files that are not kept updated are of little to no use when faced with a newly discovered virus.

Provides on-access scanning

On-access scanning allows you to setup the A/V software to scan all files, or certain key files, every time a file is read from, or written to, the hard disk.

This setting has the tendency to slow down the machine performance, but it is well worth the performance hit for the security benefit.

Provides on-demand scanning

On-demand scanning gives you the ability to perform a one-time scan on a particular file or folder that you have reason to believe is vulnerable or may have been compromised.

Allows you to schedule automatic scanning tasks

Automatic scanning tasks allow you to conveniently configure scheduled scans to correspond to idle time on the PC.

Offers advanced scanning techniques (boot-time, heuristics, archive files)

Boot-time scanning will scan your hard disks boot sector each time the PC is booted up.

Heuristics analysis enables the A/V scanning engine to detect a virus based on the characteristics or behavior of the file, instead of on a known signature pattern. This gives the advantage of detecting previously unknown viruses. Unfortunately, it will often trigger false alarms, as well, as it is difficult at best to determine the intent of a piece of code.

An archive file is a compressed file that must be extracted prior to being able to read/execute it. If our A/V program can scan inside archive files, we will be able to scan the file as it is being extracted and written to disk.

Integrates tightly with your e-mail application

After automatic updating, this is probably the most important feature. The A/V product needs to be tightly integrated with our email client, presumably Outlook. For the most secure configuration the A/V software should offer an email-arrival scan with an on-demand scan. The on-arrival scan should be a continuous scan that is running in the background waiting to scan any incoming email. The on-demand scan could be a toolbar, or menu option, integrated into the email client enabling us to scan our inbox, or any other folder, as desired.

Provides configuration locking

Finally, the A/V software should provide us the ability to lock our configuration settings, thereby restricting changes to authorized persons. We do not want our users, children, or malware to be able to change settings or disable the product.

We have another crucial layer of defense in place. Our antivirus software is running in the background proactively scanning all files read from, or written to, the hard disk. We know that our email is being securely monitored, and we have the ability to run a scan on our system whenever we feel the need to do so.

However, what can we do about the system/application vulnerabilities that the worms are targeting?

Patch Management

Overview

August 2003 saw a flurry of Internet worm activity. No less than four significant worms exploited weaknesses in Microsoft Windows Operating Systems (OS). On August 01, a mass-emailing worm named Mimail was discovered in the wild; on August 11, MSBlaster infected more than 100,000 vulnerable systems within its first day; and on August 18, both MSBlaster imitator Welchia, and yet another variant of Sobig, Sobig.f, were discovered.

What did all of these worms have in common? All four of them exploited well-known operating system vulnerabilities that had security patches available long before the worm's release. A study, which correlates nearly 1.5 million scans from vulnerability-assessment company Qualsys over an 18 month period, revealed that better than half of the vulnerable systems are still unpatched 30 days after a patch is released.^{***} Had the available patches been applied when made available, the effectiveness of these worms would have been significantly diminished.

Largely because of its market dominance, Microsoft has been the focal point of the vast majority of the discovered vulnerabilities. To assist their users in the alleviation of these vulnerabilities, Microsoft have developed various update solutions. We will look at two of them targeted to the small businesses and home users.

Windows Update

Windows Update is an online repository of OS, software, and hardware patches for Windows 98/Me/2000/XP/2003. Microsoft presents the following directions for using the Windows Update process^{†††}.

1. Using your web-browser, navigate to <http://windowsupdate.microsoft.com> and click the "Scan for updates" button
2. Scroll through all of the available updates in each of the "Critical Updates and Security Patches", Operating System, or "Driver Updates" categories and click on the Add button to select the individual update and add it to the collection of updates to install. A full description of each item is available for review
3. When all required updates are selected, click Review and install updates, and then click Install Now.

^{***} Lemos, R. (2003). Study: Bad security flaws don't die, CNET Networks, Inc.

^{†††} Microsoft (2003). Understanding Patch and Update Management: Microsoft's Software Update Strategy, Microsoft Corporation.

An alternative to this manual three-step process for users of Windows 2000 SP-3, and Windows XP SP-1, is to configure each system to automatically update via the Automatic Update (AU) client.

Software Update Services (SUS)

SUS is, in effect, a local version of the Windows Update repository. SUS requires a Windows 2000/2003 server with Internet Information Services (IIS) running on it. The SUS server synchronizes with the official Windows Update site and pulls down the patches that are available for the operating systems that the administrator selects. In turn, the AU client, configured on each PC on the network, gets updates from the SUS server. The benefit of this solution is that the administrator schedules synchronization during off peak hours, and approves or denies patches on an individual basis. The desktop PCs will only install the pre-approved patches.

Recommendation

For the home user, Microsoft's Windows Update solution is an excellent means to ensure proper maintenance of security patches. This option requires the least amount of knowledge and effort from the user with the burden falling on Microsoft to analyze the PC's needs and provide the necessary updates. If the home user operating system supports the Automatic Update client, then the user can configure the patching process to take place automatically without any manual intervention. Alternately, the user can configure Automatic Update client to simply give notice of the patch availability, or to download the patch and prompt for installation when convenient. If the OS does not support AU, then the user must regularly visit the Windows Update web site to initiate a system scan and subsequent patch installation.

For the small office, Microsoft's Software Update Services offers the administrator the ability to easily deploy any security patches or critical updates to any Windows 2000/XP/2003 computer on the network. Moreover, the administrator can selectively approve only the patches that apply to their environment. A couple of added benefits to this solution is that security patches and critical updates can be deployed to computers that do not have Internet access, and network bandwidth utilization is reduced on shared, or metered, internet connections.

In addition to these update services, Microsoft provide a Security Bulletin Notification Service that both the home user and the small business administrator should be subscribed to no matter which of the other options are implemented.

Microsoft describes the communication service:

“The Security Bulletin Notification Service enables customers to receive timely and accurate information directly from Microsoft about worms, viruses, and other security events. It represents one of the first steps taken to help customers determine if an event is relevant to their environments, how and when to download and deploy the security

patches, and how the software updates or security patches affect their overall IT infrastructures. Customer can sign up to be notified via e-mail when the latest Security Bulletins are posted with versions for IT professionals and end users.”^{†††}

Recently, Microsoft have rewritten the Security Bulletins to take the home user and the more experienced admin into account. The bulletins targeted to the home user contain more user friendly language and explanations. As you might expect, the admin version of the bulletin is more technical in nature. I strongly recommend that you subscribe to the appropriate bulletin; they are an excellent resource for better understanding the patch process.

A Deeper Look

Worms

Mimail

Spread via mass-emailing. The email was purportedly from the user's system administrator informing the user that their email account was about to expire and to read the details in the attached file. The file attachment was a worm that exploited two known MS weaknesses ([MS02-015](#), [MS03-014](#)) to harvest a listing of email addresses from the users system and subsequently email itself to the addresses in the listing. MS02-015 was originally posted March 28, 2002 and subsequently updated on May 09, 2003. MS03-014 was originally posted April 23, 2003.

Network Associates, Inc. provides excellent details regarding the virus's characteristics and removal instructions.

http://vil.nai.com/vil/content/v_100523.htm

MSBlaster:

Targeted a flaw in Microsoft's Remote Procedure Call (RPC) protocol ([MS03-026](#)). The worm attack vector was to scan random Internet address ranges for machines responding on TCP and UDP port 135. Once a machine was found, the worm exploited the vulnerability to open a remote command shell. Via the command shell, the victim computer was instructed to download the worm, and the process started all over again. MS03-026 was posted on July 23, 2003.

Once again, look to Network Associates, Inc. for excellent details regarding the virus's characteristics and removal instructions.

http://vil.nai.com/vil/content/v_100547.htm

Welchia:

Spread by imitating MSBlaster. However, the intention of Welchia seemed to be benevolent in nature. Contrary to MSBlaster, Welchia used the remote command shell to download patches from Microsoft to patch the very vulnerability it exploited. Furthermore, the worm's author included a self-elimination routine to delete itself on January 01, 2004.

^{†††}Microsoft (2003). Understanding Patch and Update Management: Microsoft's Software Update Strategy, Microsoft Corporation.

Additional detailed information can be found at
http://vil.nai.com/vil/content/v_100559.htm

Sobig.f:

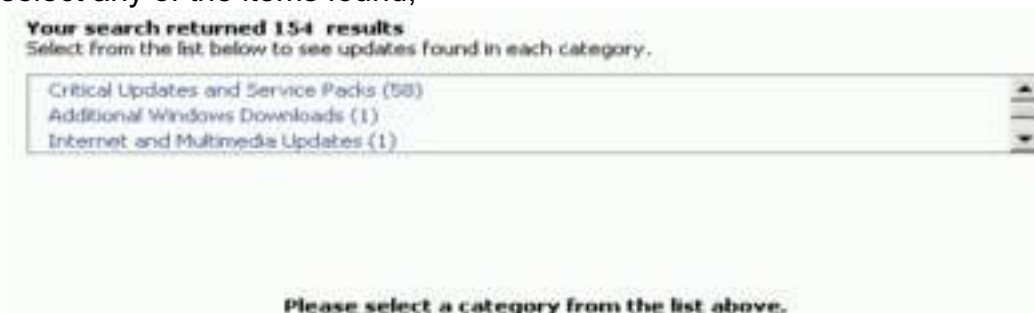
The sixth and most widespread variant of the Sobig worm. It propagated via a self contained email engine or network shares. The worm harvested email addresses from the victim's computer, possibly to be used to build an address list for spammers. The worm is capable of downloading files from a remote site and generates traffic on outbound UDP port 8998 and inbound UDP ports: 995, 996, 997, 998, and 999. Find more detailed information at http://vil.nai.com/vil/content/v_100561.htm

Windows Update

Windows Update offers two different methods of retrieving security patches and critical updates. The default approach is detailed in the Windows Update section above. The second approach is via Windows Update Catalog. The windows update catalog provides the user the ability to search for updates for individual categories and save the files to a location of their choice for later deployment. The benefit of this approach is that the user can locate all of the updates, enhancements, or device drivers for an operating system other than the one installed on their local computer. For example, a user running Windows 2000 SP4 can search for all available updates for a Windows 98 system



select any of the items found,

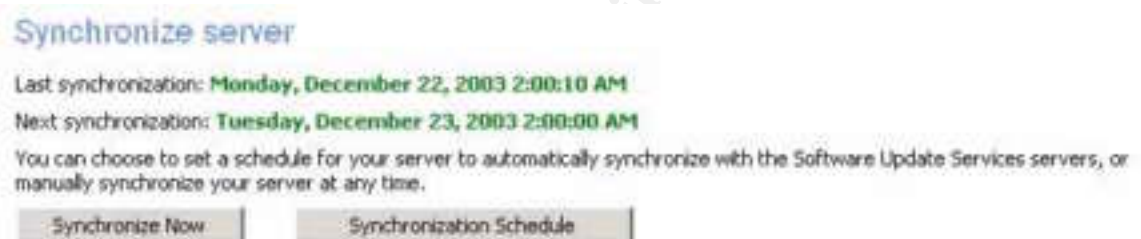


add them to the “Download Basket”, and save them to the local drive to be deployed on a Windows 98 system that cannot be connected to the internet.



Software Update Services

With SUS you can configure the server to synchronize on a schedule or manually as convenient:



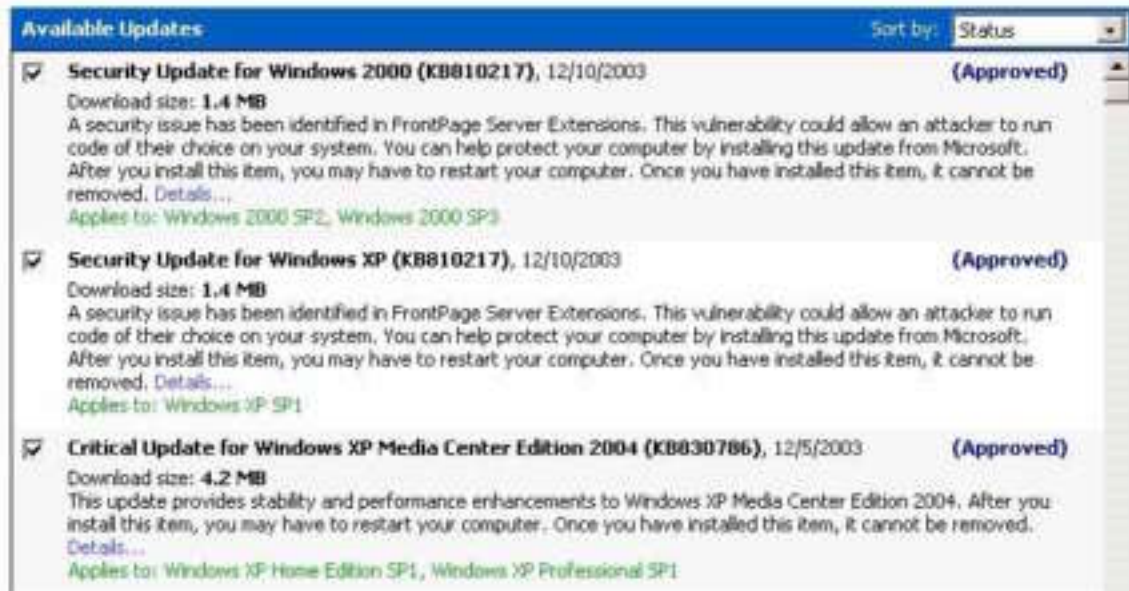
The synchronization process is logged and displays the names of any updates that were downloaded, removed, or reissued. If no changes were made, the log displays a statement indicating such.



If any security patches or critical updates were downloaded, the next step is to approve which of these the AU client will install on each PC:

Approve updates

Choose the updates that you would like to distribute to your clients, and then click **Approve**.



When network PCs, running AU client 2.2, update at the next scheduled time, they will only download the approved security patches and critical updates.

Looking to the future, in spring 2004 Microsoft will offer updated versions of the tools we have discussed. The Windows Update site will offer patches, updates and service packs for Windows 2000/XP/2003 as well as SQL Server 2000, Exchange Server 2003 and Office 2003. Microsoft's Baseline Security Analyzer (discussed in the next section) will be upgraded to provide tighter integration with SUS and Windows Update. The SUS upgrade will include improvements such as per machine/group/update reporting, install success/failure reports, and the ability to rollback to a previous configuration if an update causes adverse results.

By its very nature, software development can be quite complex. Although I am of the opinion that more can be done to make sure that software is developed in a more security conscious manner, the fact remains that many common vulnerabilities are only discovered after the product has been on the market for a while, thus in wide-spread use. Most software vendors readily prepare patches for known issues with their products. Unfortunately, there is a critical period between the time the vulnerability is publicly known and the time the vendor releases a patch. Therefore, it is vital that the SOHO user keeps informed of any known issues with the software installed on their systems and applies the appropriate patches as soon as practical. Failure to do so can result in systems being compromised and/or private data being accessed.

To this point, we have secured our perimeter to allow only authorized network access; we have installed antivirus software to help ensure our authorized traffic plays nice with our systems, and we have patched the known operating system

and application vulnerabilities. What can we do to help secure our environment from new exploits targeting our systems?

Operating System Hardening

Overview

As we have previously discussed, for various reasons, Microsoft's operating systems rank as the most vulnerable, therefore exploited, systems. Fortunately, there are steps that you can take to mitigate many of these vulnerabilities beyond security patches and critical updates.



As it turns out, not all of the services and files installed in a default Microsoft OS installation are necessary or required for daily operation. The trouble is in determining which services and files to eliminate on our systems for our given situation. We all use our systems to accomplish different tasks, therefore there is no universal service disabling setting that applies to all systems.

Keeping to our theme of security within the SOHO budget constraint, I would like to expose you to two tools that Microsoft provides free-of-charge to assist in hardening our computers. Certainly, there are excellent third-party tools that offer more features than these tools from Microsoft, however, none of these compare in price.

Microsoft Baseline Security Analyzer

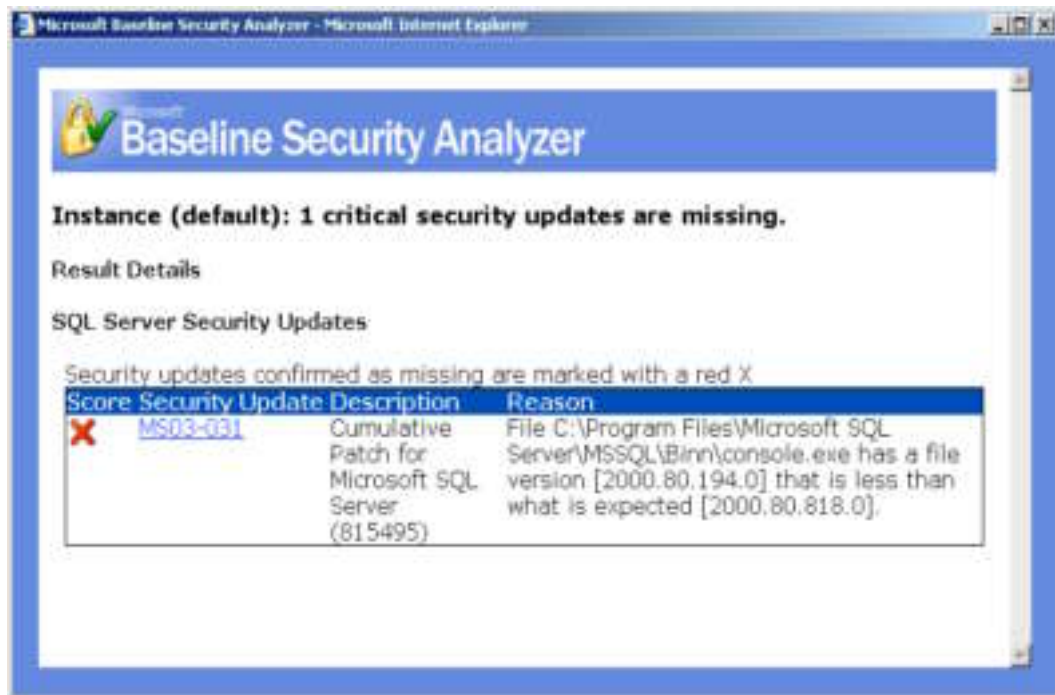
For the small business administrator and individual home user alike, Microsoft's Baseline Security Analyzer (MBSA) allows you to perform a security scan on a single computer, a domain, or an IP address range. MBSA scans for vulnerabilities in Windows, IIS, and SQL; weak passwords; and missing security updates.

By default the security update scan runs against the listing of security patches and critical updates from the Windows Update site; however you have the option to run it against the pre-approved-patch listing on a local SUS server if you have SUS configured. More specifically, MBSA scans for missing security updates in Windows NT4/2000/XP/2003, IIS 4.0 and 5.0, SQL Server 7.0 and 2000 including MSDE, Exchange 5.5 and 2000, IE 5.01 and later, and finally Windows Media Player 6.4 and up. Each scan generates a thorough report for each PC scanned explaining each result, assigning a severity level and offering recommended corrective action.

Scanned with MBSA version:		1.1.1
Security update database version:		1.0.1.507
Security assessment:		Severe Risk (One or more critical checks failed.)
Security Update Scan Results		
Score	Issue	Result
	SQL Server Security Updates	Instance (default): 1 critical security updates are missing. What was scanned Result details How to correct this
	Windows Security Updates	1 security updates are out-of-date. What was scanned Result details How to correct this
	Windows Media Player Security Updates	1 security updates are out-of-date. What was scanned Result details How to correct this
	ITS Security Updates	No critical security updates are missing. What was scanned
	Exchange Server Security Updates	Exchange Server is not installed.
Windows Scan Results		
Vulnerabilities		
Score	Issue	Result
	Password Expiration	Some unspecified user accounts (7 of 9) have non-expiring passwords. What was scanned Result details How to correct this
	File System	All hard drives (3) are using the NTFS file system. What was scanned Result details
	Autologon	Autologon is not configured on this computer. What was scanned
	Restrict Anonymous	Computer is running with RestrictAnonymous = 2. This level prevents access to any resources that do not have explicit permissions set for the Anonymous account. What was scanned
	Administrators	No more than 2 Administrators were found on this computer. What was scanned Result details
	Local Account Password Test	This check was skipped because user chose not to perform password checks during the scan.
Additional System Information		
Score	Issue	Result
	Auditing	Enable auditing for specific events like logon/logoff. Be sure to monitor your event log to watch for unauthorized access. What was scanned How to correct this
	Services	Some potentially unnecessary services are installed. What was scanned Result details How to correct this
	Shares	7 share(s) are present on your computer. What was scanned Result details How to correct this
	Windows Version	Computer is running Windows 2000 or greater. What was scanned
Desktop Application Scan Results		
Vulnerabilities		
Score	Issue	Result
	IE Zones	Internet Explorer zones do not have secure settings for some users. What was scanned Result details How to correct this
	Outlook Zones	Microsoft Outlook 2002: Some security issues were found. What was scanned Result details How to correct this
	Macro Security	4 Microsoft Office product(s) are installed. No issues were found. What was scanned Result details

Simply click on any of the hyperlinks to see detailed information regarding that particular vulnerability. For example, if you were to click on the "Results detail"

link under the SQL Server security updates section of the sample report, you would see the following detailed information:



One click on the MS03-031 hyperlink will open your web-browser to the Microsoft security bulletin specific to this issue. All the details about the vulnerability are here as is the required patch.

Security Configuration Manager

Security Configuration and Analysis enables you to view the current security configuration on your computer, and to alternately set different, or additional, security parameters as necessary. The tool enables you to manually alter the numerous security settings, or import predefined security templates. Moreover, you can export the settings of an ideally configured computer to be used as the template for all the remaining computers on your network.

Security Configuration and Analysis presents highly granular configuration control on the individual system. Running an analysis reveals highly detailed information about all security aspects of the system. Furthermore, the analysis can reveal configuration errors that may have occurred over a period.

Several of the system specific templates provided:

Default workstation	basicwk.inf
Default server	basicsv.inf
Default domain controller	basicdc.inf
Compatible (w/NT) workstation or server	compatws.inf
Secure workstation or server	securews.inf
Highly secure workstation or server	hisecws.inf

Recommendation

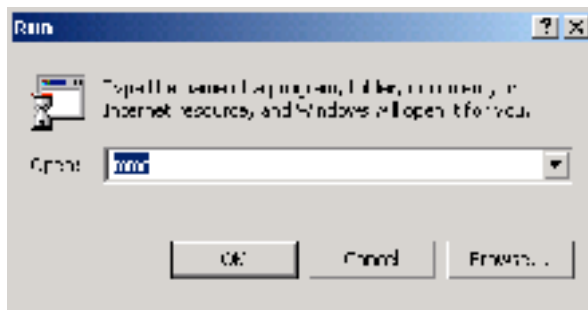
Download MBSA and depending on your individual situation, install it on your PC, or install it on a central server.

MBSA is available for download at:

<http://download.microsoft.com/download/8/e/e/8ee73487-4d36-4f7f-92f2-2bdc5c5385b3/mbsasetup.msi>

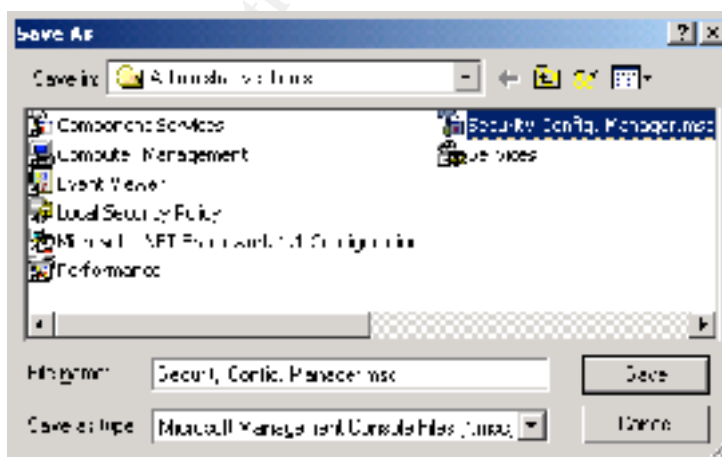
The Security Configuration and Analysis tool is already installed on the PC, however, you will need to complete the following steps to configure the tool to be able to launch from the Start menu:

Left click on the Start button, click on Run, in the Run dialog box type mmc and press enter,



On the Console1 window press Ctrl-M to launch the Add/Remove snap-in option, Click the Add button, in the Add Standalone Snap-in window scroll down till you find Security Configuration and Analysis snap-in:

Click the Add button, then the Close button, then the OK button. The Security Configuration and Analysis snap-in will appear in the Console1 window. Click the Console menu-option, then click Save As and in the dialog box give the Console1 window an appropriate name and click the save button:



Follow the directions displayed on the ListView to begin the Security Configuration and Analysis process.

After you have installed MBSA and configured the Microsoft Management Console (MMC) with the Security Configuration and Analysis tool, you should run the MBSA scan and carefully review the results. Hyperlinks provided for each category on the report will guide you through the process of patching your system. If the report displays any items under the Windows “Vulnerabilities” and “Additional System Information” headings, and it will, you will be able to rectify the vast majority of these items when you apply the “Secure workstation or server” template in the Security Configuration and Analysis described console in *A Deeper Look*. Any items listed under the individual applications sections of the report will have hyperlinks to detailed instructions to guide you through the necessary steps required to mitigate the reported vulnerability.

A Deeper Look

Microsoft Baseline Security Analyzer

When MBSA is run for the first time, it downloads a copy of mssecure.xml. The XML (Extensible Markup Language) file contains information about which security updates are available for the particular products that MBSA scans against.

MBSA parses the XML file to determine what security updates are available for your particular combination of software. Three criteria determine which security updates apply to your situation: registry key associated with the requisite update; the file versions; and the checksum for each file in the update. When checked, if any of these three criteria fails, the update is considered missing and MBSA will flag it as such in the report. The report will have hyperlinks leading to detailed information regarding “What was scanned”, “Result details”, and “How to correct this”. The “What was scanned” page displays what Microsoft calls the “Check description” describing both the scan performed and the vulnerability. The “Result details” page displays a link to the official Microsoft bulletin issued for the vulnerability. The “How to correct this” page displays step-by-step instructions for mitigating the particular vulnerability.

In addition to the GUI version of MBSA, Microsoft offers a command-line version of the tool. The command-line version (mbsacli.exe) is typically used when an administrator desires to automate redundant tasks via command file scripts. To generate output similar to the GUI reports, the command line tool needs the following switches when executed: /baseline, /s, and /nosum. The /baseline switch tells the tool to scan for updates marked as critical, the /s switch tells the tool to suppress security update check notes and warnings, and the /nosum switch tells the tool to skip the checksum as it can be very time consuming.

Microsoft created a MBSA whitepaper that details every intricacy of this tool. Please take a moment to read this document to become familiar with all the functionality of the tool along with explanations of the various vulnerabilities that are checked.

<http://www.microsoft.com/technet/security/tools/mbsawp.asp>

Security Configuration and Analysis

The first time that you run Security Configuration and Analysis, you will need to set a working database. This database can be an existing personal database that you copied from an already properly configured computer, the default database supplied with the tool, or a new database that you are creating for your settings. If the database that you choose is not the database that was used to configure your current settings, then you will be prompted to import a security template.

While your individual situation will dictate which template is more appropriate, and, which settings need additional attention, I recommend that you begin with the “secure workstation or server” template, `securews.inf`. When applied, the settings of the “secure workstation or server” template implement all of the recommended security settings for all system areas that are not considered secure by default (note: only the file system and registry is considered by Microsoft to be secure by default). To apply the configuration of your imported template, right-click on Security Configuration and Analysis and select “Configure computer now”, when prompted choose a log file to record any errors. When the configuration process has completed, your new settings will be in place. I strongly recommend rebooting the system to make sure all changes have taken effect.

The Help Topics available in the Security Configuration and Analysis console help to better explain the tool functionality and will offer distinctions between the various pre-defined templates. It is well worth reviewing.

Depending on the environment, when I “lockdown” a customer’s network I use these tools I have just described. However, I do not use them as provided. Instead, I have modified the templates to conform to what I have read through the Windows hardening guides that have been published by highly respected security agencies/companies such as the NSA and SANS. Furthermore, Microsoft also offers a hardening guide. The Microsoft guide, in particular, comes with seven additional templates that reflect the necessary changes needed to further harden your system. I highly recommend that you review these guides. I have included a template, similar to the one I use for member workstations, in Appendix B.

Finally, after having discussed hardware, software, and utilities, we come to what I consider the most integral part of securing *any* computing environment: the user.

User Awareness

No other component, no other layer-of-defense, can more profoundly impact the security of our Information Systems than the persons that we have operating these systems. Information security requires constant vigilance, it requires continuous education, and it requires a lot of dedicated time, and I am only speaking of what is required of those us that are employed in the field.

Imagine, then, what it must be like to be a system user that is getting paid for some *other* job.

Fred works for a local title company. Fred needs to access a local-government auditor's-office website to retrieve required tax information. This is the first time that Fred has had to go to this particular county's website; as such Fred is unfamiliar with the site. As luck would have it, the county website is simply www.nameofcounty.gov. Fred registers for an account to access the site and receives an e-mail with the username and password. Attached to the email is an "taxation-data-privacy" document and in the text of the email Fred reads a note indicating that he must read and agree to the document before he can access the county tax data. Fred opens the document and within seconds the mortgage center's network is brought to a screeching halt from what will forever be known as the FredOverInTheTitleOffice worm.

Now, Fred did not intend to disable the network. In fact, Fred was simply going about doing his job the best he can. What could *Fred* have done differently? How could we have prevented this situation?

First things first, had the network personnel followed the security administrator's instructions, there would have been an endpoint firewall and updated antivirus software on Fred's computer. The endpoint firewall would have stopped the outbound traffic from Fred's computer if the worm's payload was not identifiable, and stopped, by the updated antivirus signature files. Furthermore, had the antivirus package had the ability to heuristically view the email attachment, it would have discovered that the document file was really taxprivacy.doc.exe.

But, is that really what should have happened first? Maybe the situation could have been avoided if Fred had received the security awareness training that was stalled during development while the understaffed security department cleaned up systems from MSBlaster.

Thus, we see the paradox that is information security. Do we first install a perimeter firewall, an endpoint firewall, antivirus software, operating system patches and disable unnecessary services? Or, do we first teach Fred how to recognize sham websites and email attachments with multiple extensions?

It is my belief that both things must be taken care of at the same time, but by different people. The persons charged with building and configuring the systems (even if that is us at home), must be educated about the necessity of firewalls/antivirus/patches/hardening having to be in place before a system can be allowed to connect to the Internet. While at the same time, the users of these systems (again, even if this is us at home), must be educated about the perils of life plugged in to the Internet.

Before any user is permitted to log on to a workstation, whether in the office, or at home, that user should be required to have Internet Awareness training. The training should include, at a minimum, the following topics listed in Table 3:

Passwords

Passwords should be strong but easy to remember.

- A strong password has at least 8 characters and mixes upper and lower case letters with numbers and special characters. For example, this password is secure and easy to remember: "Ez&hTwoGs" Easily remembered by the phrase "Easy and hard to guess"
- Never write your password down unless it will be locked out of site in a location that only you have a key to.

Email

- Never open *unexpected* email attachments. If the attachment appears to be from a known source, but is unexpected, scan it with you virus scan product and/or contact the sender to verify they sent an attachment.
- Never click on unexpected hyperlinks embedded in email messages.
- Be very considerate of what you write in your email, this digital form of your words is virtually permanent. Once you have sent an email, it does not matter whether you, or the recipient has deleted the message, copies of it can be anywhere on any email server/relay between you and the recipient.

Web Browsing

- Take care to only visit reputable or trusted sites. Merely visiting a nefarious site can spark a system compromise.
- Never click on the Pop-up Advertisements. Many of these are known vectors of spyware and adware contamination.
- Never download games or shareware without verifying their source
- Be very careful when typing URL names:
www.whitehouse.com is an adult entertainment site, not the United States White House website
(www.whitehouse.gov)

Social Engineering

- Never share your password with *anyone*. Your password is linked to your username name, and you will be held accountable for all activities linked to your username.
- Be very careful what information you give out over the phone. Anyone can call your office and purport to be someone in IT that needs certain data. Ask the caller to visit your office where you can verify her identity.

Table 3: User Awareness Topics

This listing is by no means all-inclusive. Many other topics and sub-topics are discussed in standard Information Security Awareness training when delivered by

a professional company that specializes in this arena. Alas, we are still dealing with SOHO budget constraints; consequently I include this short list and strongly encourage the reader to visit sites such as www.sans.org/awareness to pursue comprehensive, cost-effective Information Security Awareness training.

Conclusion

There we have it, defense-in-depth.

We began with a single computer connected to the Internet via broadband. In between here and there, we discussed the need for a perimeter to core security solution. We began our discussion with dialog describing the need for a hardware-based firewall/router device.

Once we had the perimeter secured, we found that we still were not as safe as we could be. We developed another layer of defense to backup our perimeter defense, after all we still needed to deal with legitimate network traffic. Thus, we deployed endpoint firewalls and strong antivirus software. While discussing the antivirus software, we pointed out that the most important part of the antivirus product is the signature files and those were virtually ineffective if not kept updated on a daily basis.

By this point we had taken care of a great many of the threats to our systems and data, but what about the operating system software controlling the systems themselves? The complexities of the operating system software, along with the limited environment that the software could be exposed to while testing, lead to vulnerabilities being discovered and subsequently exploited. We determined that we needed yet another defensive layer in place to mitigate these vulnerabilities. It was our good fortune that the developer of the operating system also provided free tools to determine the vulnerabilities on our system. Moreover, the free tools led us to where the fixes to these vulnerabilities could be found.

After dealing with the vulnerabilities of the operating system software, and installed applications, we found that we must reconfigure several of the default system settings. These settings were less than secure and, once again, we found that the operating system developer also supplied tools to alleviate these system-settings shortcomings.

Finally, after having so confidently secured our environment, we saw a scenario where during the normal use of the computer system, a user still had the ability to bring our network down. Therefore, we determined that we needed to train our user on the safe use of the systems and applications.

We have come a long way, and covered a lot of material, quite frankly, more material that I had initially anticipated. As I developed this document, I discovered that each of the topics that I covered could be, and most like are, full whitepapers in and of themselves. However, I felt that it was extremely important that ample consideration be given to each of the topics as I truly believe that each of these layers of defense must be in place if we are to keep our systems and data safe and secure in our SOHO environment.

Once again, follow the links, read the materials available, continue to read, and attend some training courses. We will all be glad that you did!

© SANS Institute 2004, Author retains full rights.

Appendix A - Description of Malware Terminology

Malicious Software - Malware

Malware is generally considered any software that attempts to perform any malicious activity on your computer be it deleting files, sending private information to the Internet, etc. Viruses, worms and Trojan horses are commonly referred to as malware.

Viruses

The computer-virus web page at faqs.com defines a computer virus as "...a program designed to spread itself by first infecting executable files or the system areas of hard and floppy disks and then making copies of itself. Viruses usually operate without the knowledge or desire of the computer user."§§§

Given that a virus is a software program, a virus can affect your computer in any way that any other software program can. System files can become corrupted; can be deleted; can be renamed. Moreover, viruses can download other nefarious files; or install Trojan programs.

Worms

Worms, like viruses, are malware. However, unlike viruses, worms do not "infect" files with their malware. Instead, worms simply replicate themselves across network shares, via mass emailing or by scanning the Internet for vulnerable computers.

Trojan Horses

Trojans are programs publicized as one type of file (free game, helpful tool, etc), but really are an altogether different file, often times malicious. For example, the cool tool that you downloaded to clock your Internet speed turns out to be a key-logger with its own SMTP (email) engine that sends your passwords and credit card number to the author.

Spy Software – Spyware

Spyware is just what the name implies – software that spies on a user. Spyware monitors and logs keystrokes, web browsing, instant messaging dialogue, chat room dialogue, etc. If you can execute it on a PC, spyware can log it. Spyware runs behind the scenes, so to speak, and it is difficult to distinguish without special tools. In addition to being malware, often times you can find spyware sold as commercial software. Products to monitor a possible wayward spouse or a disobedient child are nothing more than spyware. Fortunately, many free and commercial tools exist to detect such activity. An excellent "donation ware" tool that I like to use is Spybot Search & Destroy from Patrick M. Kolla at www.safer-networking.org. Although donation ware, the product is fully functional whether you contribute or not.

§§§ Nick, (2003) Computer Virus FAQ for New Users.

Advertisement Software - Adware

Adware is different from spyware. Adware is used more for tracking your web surfing habits and tailoring web advertisements to those habits. Adware will also generate pop-ups and pop-unders to provide product advertisement. Adware is usually installed without permission, but sometimes it is bundled as part of a “free” download and may be referenced in the fine print of the End User License Agreement (EULA). You *do* read all EULA’s before you agree to them, right? Spybot S&D will remove adware as well, and I like Ad-Aware from Lavasoft at www.lavasoftusa.com.

© SANS Institute 2004, Author retains full rights.