Global Information Assurance Certification Paper

THE VALUE OF SECURITY AWARENESS TRAINING IN RELATION TO ASSET EXPENDITURES ON COMMERCIAL SECURITY PRODUCTS

Michael A. Cokenour
SANS GSEC PRACTICAL ASSIGNMENT
18 Septemebr 2003
Version 1.4b
Option 1: Research on Topics in Information Security

MONEY FOR NOTHING

Michael A. Cokenour
18 September 2003

ABSTRACT

A little over a year ago, The Gartner Group released a study ("Don't Fund Security Awareness Until You are Secure", 16 September 2002, http://www3.gartner.com/DisplayDocument?doc_cd=109981) that concluded the selling of security awareness services by consulting firms was an unsuitable use of information security budgeted funds. The area of highest priority for the appropriated INFOSEC dollars, according to The Gartner Group, was to focus expenditures on commercial applications and hardware solutions that could enforce security and lockdown vulnerabilities. Overlooking or downplaying the importance of an employee security awareness and education program is simply reckless.

In support of my contrasting position, this paper will explore a situation where a corporation expends funding on security software; yet, a lack of security awareness leads to the possible compromise of an entire enterprise. We'll examine an example of a simple internal security design error in another industry defeating the formidable physical perimeter security; we'll observe the parallel with InfoSec. Finally, some of the tools that can be found at little to no cost will be briefly highlighted. These tools can save you funds that you may use for your security awareness program.

THE CHIKEN AND THE EGG

In formulating the idea for this paper, it was not Gartner's study that inspired me to take on a paper on security awareness and ways to strengthen security on a budget (I believe the two are tied together as I find much of your security awareness is provided without cost just from meetings, memorandum, emails, knowledge transfer sessions with users and staff.) While speaking with colleagues in regards to each of the following incidents, the discussion turned to security awareness. I happened to recall Gartner had previously released a study, so I delved back into the archives and decided to rebuke much of the meat of Gartner's finding.

Unfortunately for businesses, looking at the data published in a June, 2003 Information Technology Association of America (ITAA) survey (http://www.itaa.org/news/pr/PressRelease.cfm?ReleaseID=1055867633), U.S. corporations seem to be in-step with Gartner's advice. The ITAA survey shows that forty-nine percent of information technology professionals surveyed do not believe their organizations are doing a good job at providing training and information on information security. Gartner's premise of overlooking the training aspect and going right to expenditures on tangible security resources is flawed. In doing so, an organization can

potentially create a less secure, less stable and less productive environment for their corporate assets.

When funding currently will only allow for a "one or the other" approach, an organization who wishes to make an immediate imprint on its security posture, would be wisest to first train employees in information security awareness. Upon heightening the staff's level of awareness and general security knowledge, many measures for a greater security footprint may be implemented by the trained information technology staff at little cost on the dollar of the commercial tools.

AN ENCOUNTER WITH AN "UNAWARE" CONTRACTOR

As we proceed through this first "incident", I will do my part to impart a bit of free security awareness on the user by outlining these events with the six steps of incident handling which I learned through SANS.

Preparation

Having an "Emergency CD" (or CDs) updated and ready at all times is the duty of any responsible security or system engineer. The CD should contain tools, utilities and other software that would be used to assist you in the identification, containment, eradication and/or recovery from events that require your intervention. By having my Emergency CD, I was able to handle the following situation that unfolded as I encountered a member of the contract staff that lacked proper security awareness training.

Identification

On 31 July 2003, notice arrived that there had been repeated failed logon attempts to one of our more sensitive Windows 2000 servers. According to the security logs on the server (SERVER01), the failed logon attempts had used the account "Administrator" from a machine in the building. Tracking down the port for the machine, a laptop (LAPTOP01) was found and determined to match the machine name from the SERVER01 security log.

A review of the laptop, running Windows 2000 Professional, and the system log events from 24 July 2003 revealed that seven system files (hh.exe, regedit.exe, notepad.exe, iexplorer.exe, scandskw.exe, mplayer.exe, winhelp.exe) had been restored by the Windows File Protection service. These event types can result from malware on the system attempting to replace legitimate files with Trojan versions.

Digging back further in the logs, I found similar log entries dating back to 16 July 2003. The system log file then had an unexplained gap in its events dating back to 16 June 2003. These gaps can sometimes be telltale signs of intrusions on a computer.

Another sign of trouble to come was the noted lack of any antivirus software on the

system. Also, the owner of the laptop had previously disabled all the rule sets on her firewall. Her firewall policy was therefore, "Log; but, allow all". Since there was no antivirus on the system, this was an extremely vulnerable machine.

Given the behavior with the file replacement and the lack of antivirus, I thought this was likely to be a W32/Bugbear.B infection on the laptop.

Containment

One of the first steps that was done as soon as it was identified that the LAPTOP01 machine was the source of the phantom "Administrator" logon attempts was to disconnect the network cable from the laptop. As an added measure, the wireless card was ejected, even though the card did not appear to be enabled. Since the owner of the laptop was not working on any project concerning the server which showed the failed logon attempts, it was a reasonable precaution to disconnect the laptop from the network.

Eradication

From the "Emergency CD", I copied AVG free anti-virus software (www.grisoft.com) and a trial copy of SWAT-IT (www.lockdowncorp.com) to the laptop's hard drive. The SWAT-IT software was a backup to the AVG software, in case I needed to run it if the AVG software couldn't get rid of any malware.

The software required a reboot after installation; however, I elected not to reboot at this time as I did not want to lose what was in memory (just in case this turned out to be more than a common worm). Prior experience had shown me that without the reboot, the antivirus software would not delete the malware; but it might at least detect it for us. The AVG software version on the CD was a 10 July 2003 build. Since W32/Bugbear.b was released in June 2003, I made the assumption that this build should have been suitable for testing the Bugbear theory.

The AVG software completed its check and showed the presence of W32/Bugbear (it did not return a version for W32/Bugbear).

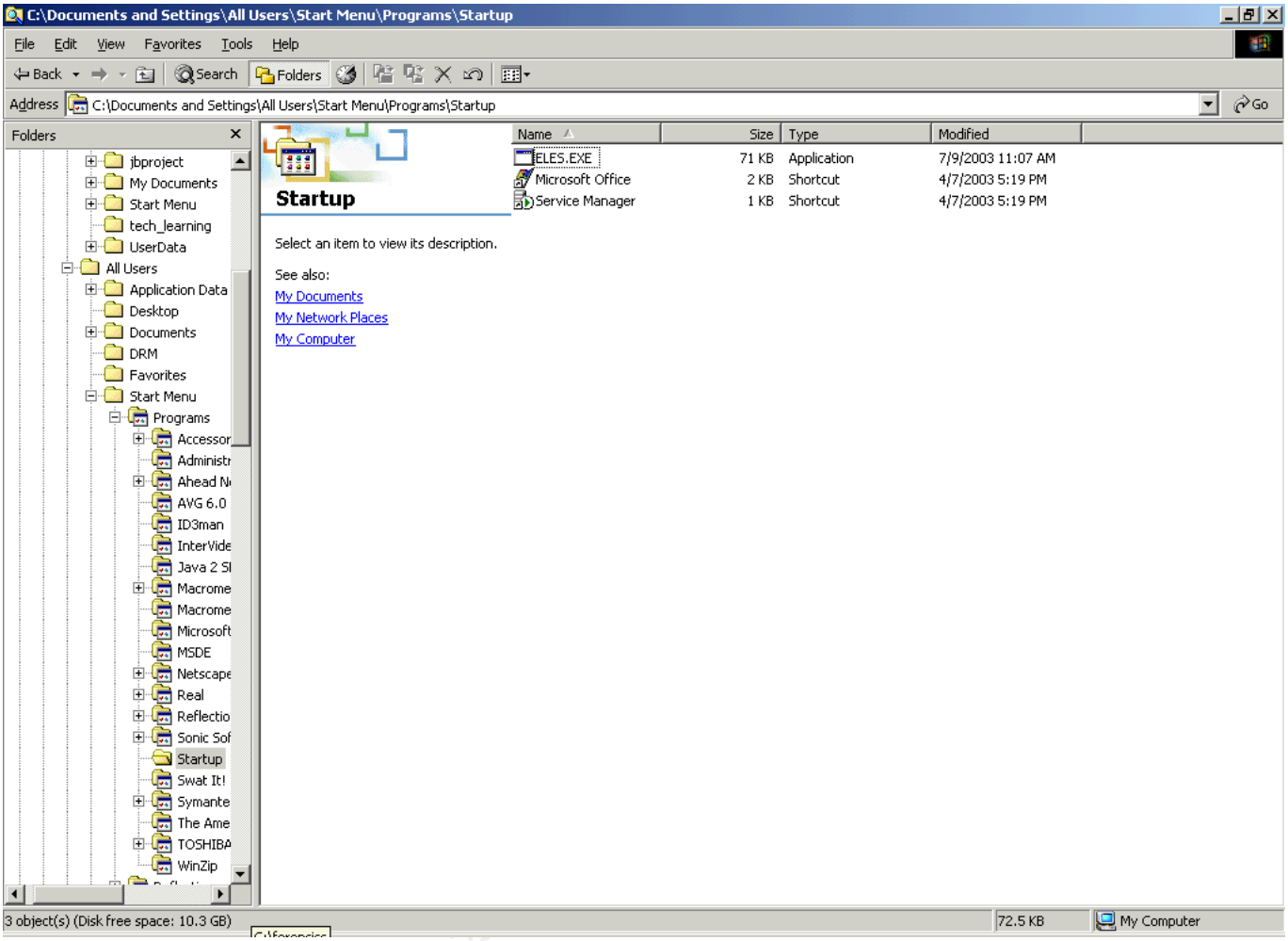
Results of Complete Test, date and time 7/31/2003 11:13:10 :

Testing C:\ volume SxxxxxxxA001 serial 6xxx-xxx6
C:\HIBERFIL.SYS Cannot open; not checked!
C:\Documents and Settings\Administrator\NTUSER.DAT Cannot open; not checked!
C:\Documents and Settings\Administrator\ntuser.dat.LOG Cannot open; not checked!
C:\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\WINDOWS\USRCLASS.DAT Cannot open; not checked!
C:\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\WINDOWS\UsrClass.dat.LOG Cannot open; not checked!

C:\Documents and Settings\All Users\Start Menu\PROGRAMS\STARTUP\ELES.EXE Virus found I-Worm/Bugbear
C:\Program Files\ADOBE\Acrobat 5.0\READER\ACRORD32.EXE Virus found I-Worm/Bugbear
C:\Program Files\Internet Explorer\iexplore.exe.tmp Virus found I-Worm/Bugbear
C:\Program Files\WINZIP\WINZIP32.EXE Virus found I-Worm/Bugbear
C:\WINNT\SYSTEM32\GFGOMKQ.DLL Virus identified I-Worm/Bugbear

Test finished, duration 00:44:13.6 s
79688 objects tested, 5 found infected

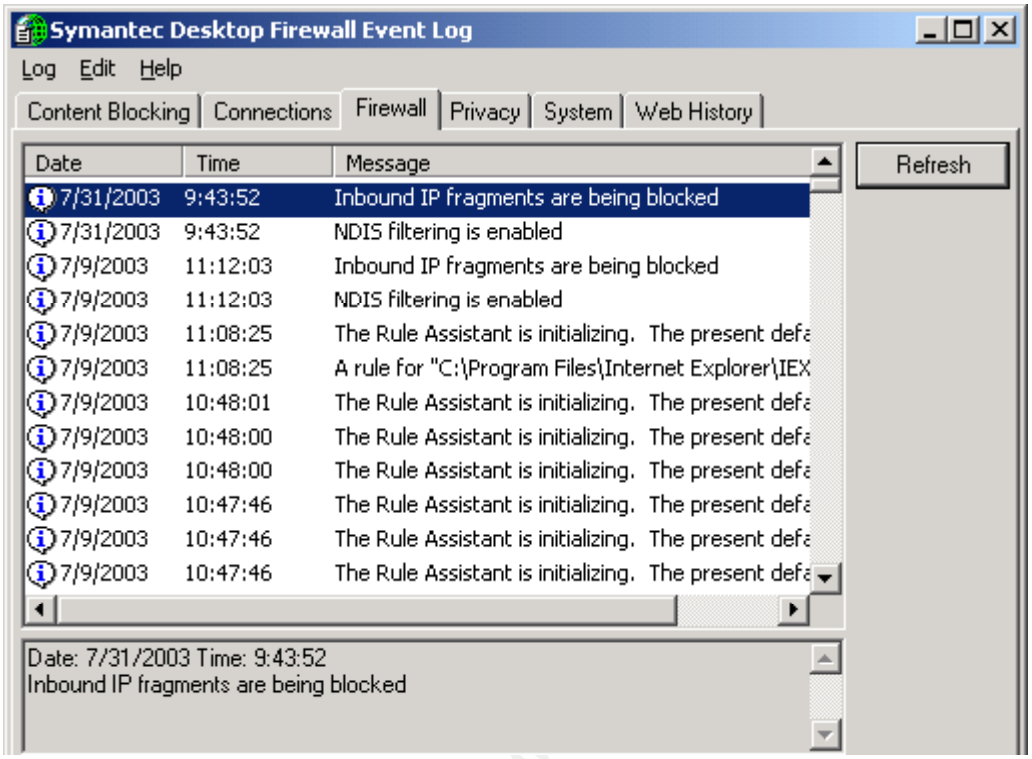
Reviewing the results of the scan above, it appears as though several of the application files (winzip32.exe, acrord32.exe, realplay.exe) had been infected. Note that Bugbear.B is known to install a randomly named *.EXE file in C:\Documents and Settings\(username)\Start Menu\Programs\Startup directory (http://vil.nai.com/vil/content/v_100358.htm). Below we see ELES.EXE in the same location. We also see in the above log, a randomly named *.dll file (GFGOMKQ.DLL) in C:\Winnt\System32\. This is the keystroke logger left behind by Bugbear.B. From our prior experience with W32/Bugbear.A, it tends to leave its *.dll file in C:\WINNT\System\ (although, this apparently is not a fool-proof identification method. RE: http://securityresponse.symantec.com/avcenter/venc/data/w32.bugbear@mm.html#technicaldetails).



A screenshot of the ELES.EXE file and its location.

Looking further into the issue I found that indeed a *.dat file NSREG.DAT existed in the C:\WINNT directory. This file contains the encrypted output from the keystroke logger program. The file size was 42KB and had a time of 09:47 on 31 July 2003. The time of the file was consistent with when I was told the system was removed from the network. Until that time, it is possible the worm's keystroke logger was sending data back through the network (or from the owner's home) to someone waiting to use the data captured. I advised the user of this. The user mentioned she had been doing on-line shopping and banking from her home recently. (The user elected to cancel her credit cards and change her bank account after an explanation of the keystroke logger.)

SWAT-IT Pro's trial software was run next to determine if there were any other issues (Trojans, bots) that might be on the machine, given that no antivirus or firewall blocking had been enabled. SWAT-IT detected nothing else suspicious on the LAPTOP01 machine. At that point I was confident enough to reboot the system as it did not look like we had anything more than a W32/Bugbear worm.



A look at the firewall log from the infected laptop

We can see the Symantec Desktop firewall running up until 11:12:03 on 9 July 2003. This time is approximately five minutes after the time of initial infection of W32.Bugbear.B. In reviewing the firewall log, it looks as though someone had restarted the firewall and filters, at least temporarily, at 09:43:52 a.m. (during a system administrators preliminary investigation).

In reviewing the disabled firewall rules, the firewall had previously been configured to listen and allow all traffic, in and out of the machine, on TCP/UDP 80, 81, 82, 83, 135, 443, 445, 1080 and UDP only 137, 138, 139, 1434. Since the worm, W32/Bugbear.B, contains a payload that drops a RAT (Remote Access Trojan) that sets up listening on 80/TCP and 1080/TCP, this is particularly troubling.

A quick examination of the machine was needed to determine the likelihood of the RAT being present and in use. There did not appear to be any type of a web server running on the box as an examination of the application logs did not seem to indicate this type of activity. Certainly after the running of the AVG antivirus software and deletion of the infecting files, the process did not appear (when a C:\netstat –an was executed), nor were there any services that were unusual or indicative of a web server (a version of apache is most common with this worm). I was specifically looking for port 1080 at this time. Since we had no network connection, I would not expect to see the evildoer establishing a port 80 connection. I was just curious to see if port 1080 started

listening automatically. Neither port 80 nor port 1080 was listening on this machine when the examination was conducted.

After a reboot, the LAPTOP had the fully installed version of AVG antivirus run against it. On this run, the AVG software was able to remove the infected files and confirmed and further identified the worm as W32/Bugbear.B.

According to the date and time on the ELES.EXE file, the infection began on or around 11:07 a.m. on 9 July 2003. The date and time on the GFGOMKQ.DLL was consistent with this as it showed a time of 11:08 a.m. the same day. (Curiously enough, 31 July happened to be the laptop owner's last day and I could not have the machine any longer for further analysis.)

Recovery

Circling back to the reason all of this came to light in the first place, I needed to make certain the SERVER01 box had not been compromised. I also needed to check the other servers that are on the segment and in the domain as well. The only servers in the network that had logon attempts from "administrator" on LAPTOP01 are shown below. The following data was extracted regarding first and last logon attempts by account "administrator" from the LAPTOP01 machine:

MACHINE	FIRST ATTEMPT	FINAL ATTEMPT
SERVER01	30 July 03 10:15:03 AM	31 July 03 09:12:35 AM
SERVER02	29 July 03 10:11:09 AM	31 July 03 09:12:33 AM
SERVER03	29 July 03 10:11:09 AM	31 July 03 09:12:31 AM
SERVER04	09 July 03 12:19:49 PM	31 July 03 09:12:27 AM
SERVER05	15 July 03 10:01:19 AM	31 July 03 09:10:08 AM
SERVER06	09 July 03 12:14:46 PM	31 July 03 09:07:10 AM
SERVER07	09 July 03 12:19:32 PM	31 July 03 09:12:23 AM

The earliest connection attempt we see is on 9 July 2003, the original date of the W32.Bugbear.B infection, at 12:14:46 a.m. on the SERVER06 box. The last connection attempt(s) was at 09:12:35 a.m. on 31 July 2003 (on SERVER01). The worm had gained the local administrator account and password from, LAPTOP01 and was attempting to exploit that information on other machines. (A good example of why you do not want to use the same account and password combinations on all machines in your network.) Fortunately, the IT department at the contractor's home office had no knowledge of accounts or passwords on our network.

Lessons Learned

In discussions with the contractor while looking at her laptop, I had found the root cause of the encountered issues were a complete lack of security awareness on her part. When asked why there was not any antivirus software installed on her laptop, the

contractor mentioned her company had installed it on the machine originally. She had seen what she believed to be errors popping up on the screen from the antivirus software (which with further questioning appear to have been alerts), so she removed the software. As for the firewall rules that she had disabled, the contractor mentioned she had disabled all of them because the rules were prohibiting her from working and accessing the internet. The lack of security awareness training as the principal factor became clear as she uttered the simple phrase 'I didn't know'. The real kicker to this whole event was that the contractor was an experienced IT administrator and architect.

As Robert Morris, Sr. is quoted as saying; "Any system can be insecure. All you have to do is stupidly manage it" (Cliff Stoll, The Cuckoo's Egg, Pocket Books, 2000).

COMMON SENSE IS FREE…USE IT

Years ago, I was a correctional officer at a fairly large prison. While a rookie, I was on my third day of on-the-job training and getting a tour of the institution, including the physical security. The compound was encircled by two high chain-length fences, topped with razor wire and intertwined with barbed wire. Rolls of razor wire were laid in the area between the two fences (known as the DMZ—sound familiar?). The perimeter was also ringed with guard towers every 200 yards or so. The towers were equipped with large caches of weapons. The ingress and egress points had armed guards and armed patrols roamed the perimeter at night. Within the confines of this outer perimeter were two separate facilities; a medium/high and a minimum-security facility.

A dual-use building that served as a kitchen and mess hall bisected the outside perimeter. The windows had iron bars on them and to get to the doors, one had to pass through a secured iron gate with a sentry present at all times. On one side of the multi-purpose building was the medium/high security prison. The other side was a minimum-security facility where the main gate was normally open (many of the minimum-security inmates came and went as they held jobs in the community).

During the tour, I observed the roof of the bisecting building was void of any barriers (such as razor wire; which was used on other similar buildings). It then occurred to me that because of the high pitch of the roofs of the nearby dormitories and cell blocks, there would be blind spots from the towers to observe anyone from the high-security side trying to climb over to the minimum security side. Once over-the-top, a leisurely stroll through an open gate awaited anyone trying to avoid serving a full-term. The decision to partner a minimum-security facility with the higher security facilities had a dramatic effect on the architecture and design of this complex.

Perimeter solutions that were put in place around the facilities were rendered nearly useless by the poorly planned functional design change. Many people who are familiar with firewalls, VPNs and intrusion detection can draw many an analogy from this example. Regardless of the magnitude of the expenditure on security system and

implementations, if there are not the people in place who have the awareness, training and experience to understand the systems and design, then the capital outlay can quickly be rendered valueless.

The contractor in my “Bugbear” example, through her complete lack of awareness, subverted the measures her employer had put in place to help assure security of not only the laptop; but the surrounding systems and network. In the long run for the consultants firm, better results could have been assured by providing security awareness training to their employees than having the funds spent rendered worthless due to a lack of training.

"HALT! WHO GOES THERE?"

Getting employees the proper awareness and skill training in security is imperative; yet you will still need the tools to assure a secure environment. There exist approaches to implement needed system and network change to enhance your information security footprint, yet lessen significantly the financial impact those changes can bring. As much of the data in the business world resides somewhere on Windows machines (servers, laptops, workstations, etc.) we will take a Microsoft-centric approach to our host security.

This section will also include screen shots form several products; however, this is not to be taken as one product being endorsed over another. If you do your research, you may find many other solutions that are more suitable to your environment. The screen shots are strictly to familiarize the new people to the category with the workings of software that provide a similar functionality to the one shown.

The last part of this section will also include changes you can make to your Windows 2000 Server installation that will improve your security and yet not cost you any funds. These settings have worked for me in the networks I am on; yet there are settings that can improve security even further that are not included as they may be too restrictive. Consider these a minimum baseline to get you started. You will want to roll your own.

Firewall

This is the one item that you may need to make a capital outlay on if you are not comfortable setting up Linux/Unix boxes and running bastion hosts, proxies and firewalls. You may wish to consider one of the many fine commercial firewall solutions. Listed in this section are several references for you to investigate and solve how you wish to approach a solution. These documents can give you a jump start if you do decide to head into the world of setting up your own cost-free firewall.

Remember that your first piece of perimeter protection actually comes in the form of your internet router access control lists. I consider this is a first chance at firewalling your environment.

Firewall References

Web Sites and Pages:

- Setting up Linux firewall using IPTABLES

  http://tennis.ecs.umass.edu/~czou/linux/firewall.html

- ZDNet Australia: Setting up a Strong Linux Firewall

  http://linuxtoday.com/security/2002040901026SCNT

- Installing OpenBSD to Make a Firewall

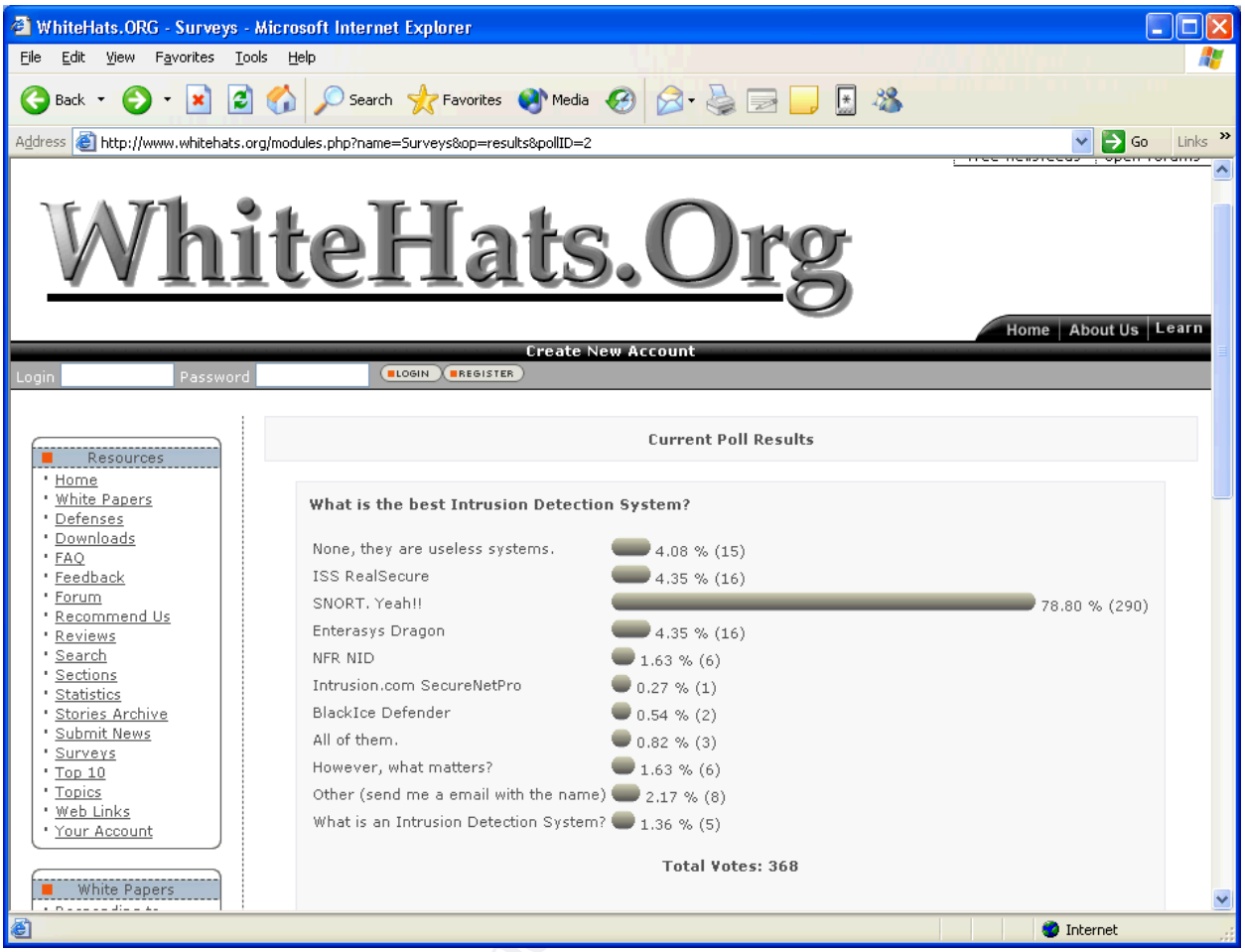
  http://www.bsdwall.org/openbsd_install.html

Books:

- Robert L. Ziegler, Linux Firewalls, 2nd edition, New Riders Publishing, 2000
- Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, Building Internet Firewalls, 2nd edition, O'Reilly, 2000
- William R. Cheswick, Stephen M. Bellovin, Aviel D. Rubin, Firewalls and Internet Security: Repelling the Wily Hacker, 2nd edition, , Addison-Wesley, 2003
- Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent Frederick, Ronald W. Ritchey, Inside Network Perimeter Security, New Riders Publishing, 2003

Network Intrusion Detection

Much has been written about the free Snort intrusion detection software and how to implement it in your enterprise. There are numerous sites and papers which will guide you in installing and using this completely customizable intrusion detection system. As an individual who has experience with both commercial intrusion detection and with Snort; I can honestly say that Snort is at least the equal of any commercial grade IDS, if not superior to all. The user community is one of the strengths of Snort. Minutes after an exploit is captured in the wild, you will find that some analyst has published a rule that will allow you to protect your network. No other IDS offers this type of speed in detection mechanisms. Nor can any commercial vendor match the helpful nature of the Snort user community to answer question you may have regarding issues with Snort or with IDS in general.



Snapshot of a poll on http://www.whitehats.org.

We will have to debate Gartner's findings regarding the overall usefulness of IDS' in general, in another paper.

I will simply leave you with one web site and a few books as references to start your studies on Snort and intrusion detection. The snort.org web site has many links to papers written to install the IDS on various operating systems and in varying network topologies. The web site also has numerous utilities and add-ons for Snort as well.

Snort References

Web page:

- Snort Home Page

  http://www.snort.org

Books:

- Brian Caswell, Snort 2.0 Intrusion Detection, Syngress Inc., 2003

- Stephen Northcutt, Judy Novack, Network Intrusion Detection, 3rd edition, New Riders, 2002

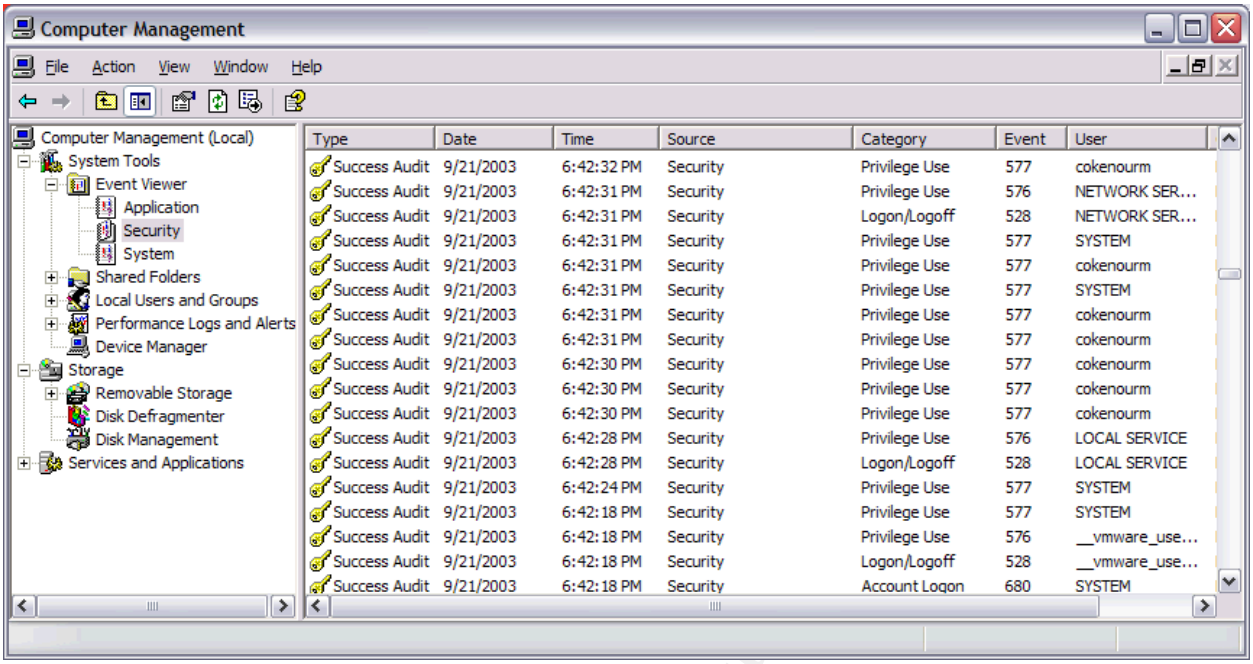
- Stephen Northcutt, Mark Cooper, Matt Fearnow, Karen Frederick, Intrusion Signatures and Analysis, New Riders, 2001

Host IDS

In a Windows environment, there is a built in Host IDS system that you must take advantage. Event Viewer is included in Microsoft Windows XP (and previous Windows versions).

Someone attempting unsuccessfully to log onto your servers and desktops will generate Event ID 529 in your Security Event log. Watching these 529's and seeing if you can find a pattern can be extremely telling. Let's say that you are pretty much a 9:00 AM to 5:00 PM type of a business. In looking through your Security Event logs, see if you have Event ID 529's appearing overnight for instance. If that is the case, see if the account name is one that is identifiable. If it is, go to that user and ask them about the events and try to determine if they were trying to logon to the system overnight. Perhaps the explanation is simple and they were working around the clock to get out a proposal. The user was prone to make mistakes due to fatigue.

(This may not always be the best approach. There is always the off-chance that the user may have been up to no-good themselves. They may have been trying to access the system in the middle of the night to pull down the marketing database or those proposals to forward to a competitor. Do a little more event reconnaissance such as looking at the log to see what they do once they have accessed the system.)



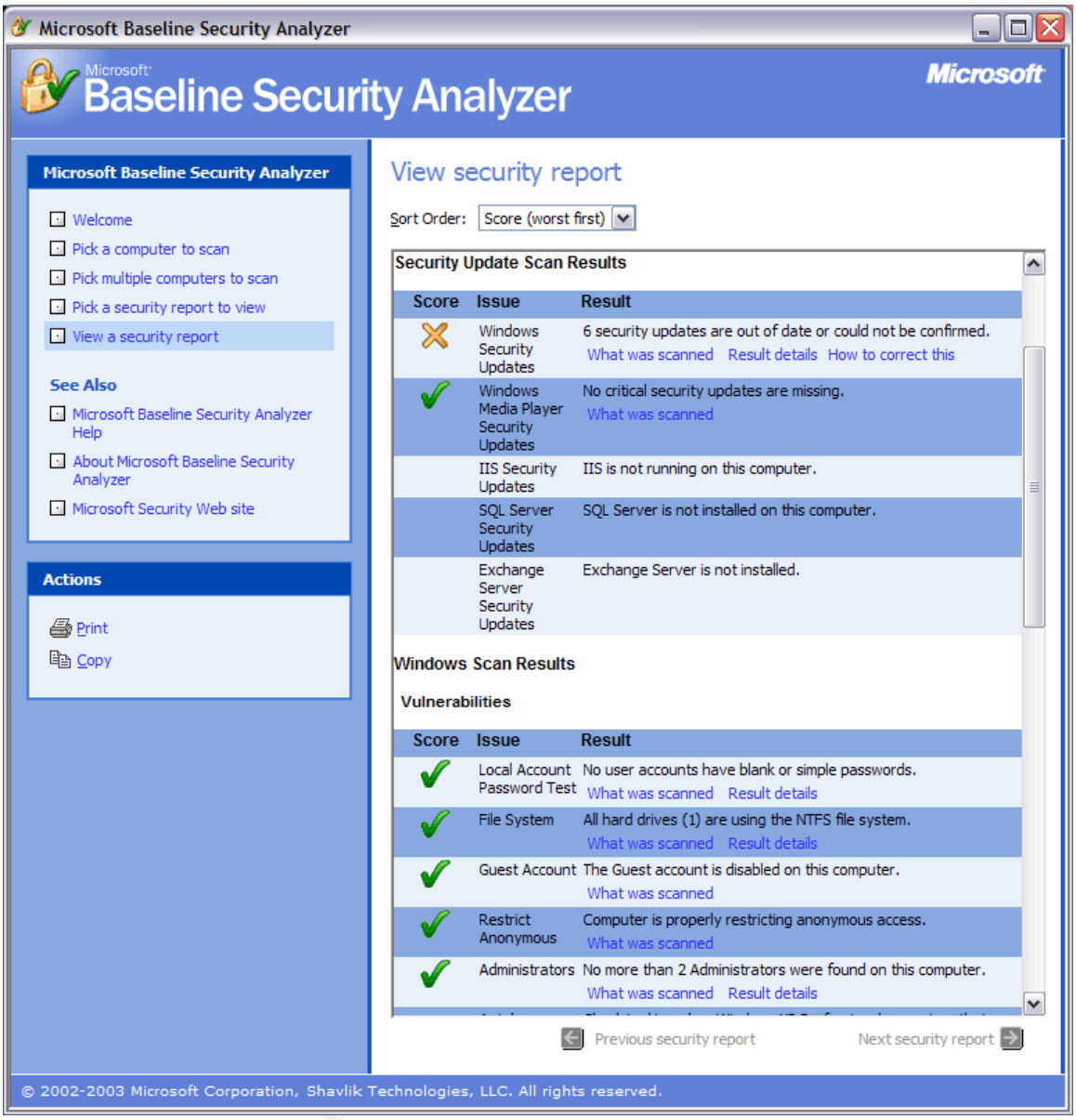
Above: A look at the Windows XP Event Viewer interface

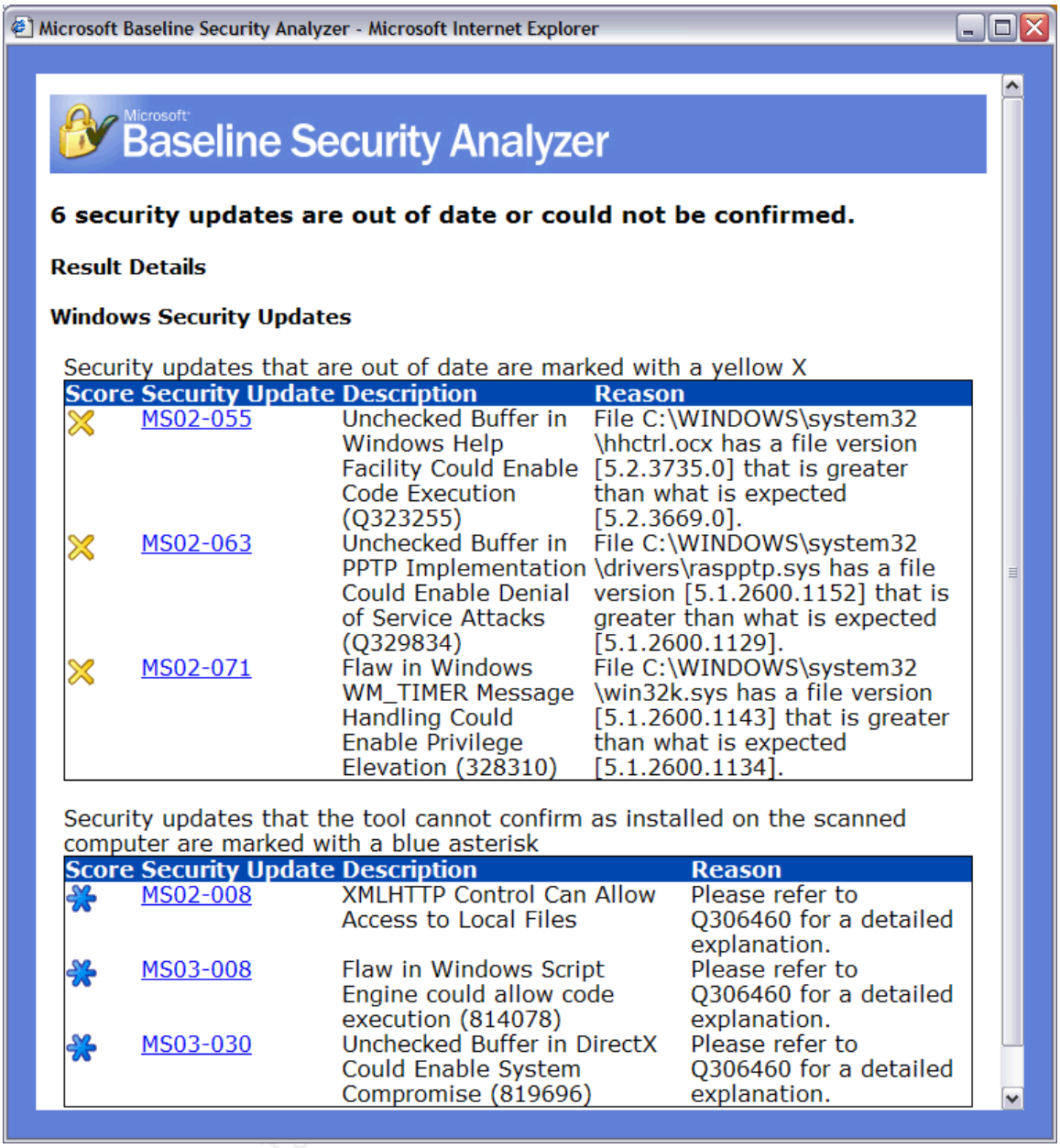
One easy, and free, tool for managing your logs is dumpel (dumpel.exe); which is included in most of the Windows server resource kits (NT and 2000).

Security Patches

In light of recent worms and the varying vulnerabilities in Windows operating systems, one of the most important “free” steps you can take in improving the security profile of your systems is to make certain all of the relevant patches have been installed.

Microsoft makes this very easy for you in fact. The Microsoft Baseline Security Analyzer is a free vulnerability assessment tool available on the Microsoft web site (http://www.microsoft.com/technet/security) that will allow you to assess the patch and service pack status of your servers and workstations. Beyond just information on patch status, this free tool also allows you to see other flaws in security such as weak passwords, account and share information and other information of interest. At the above referenced link, you will also find a list of all of the Microsoft security bulletins related to Microsoft software.





Above: Screen shots of a security scan performed on one of my laptops by Microsoft Baseline Security Analyzer.

(Note: In mentioning the recent worms in the Windows operating systems, I am not attempting to slam Microsoft. I am a proponent of Microsoft's, as well as of other operating systems, vendors and software. I believe that the more an environment has a mix of systems, the more difficult it can be to exploit. Provided the architecture is well thought-out, of course.)

TRAINING, THE FREE KIND

A good place to bring in security awareness to new employees is at the new-employee

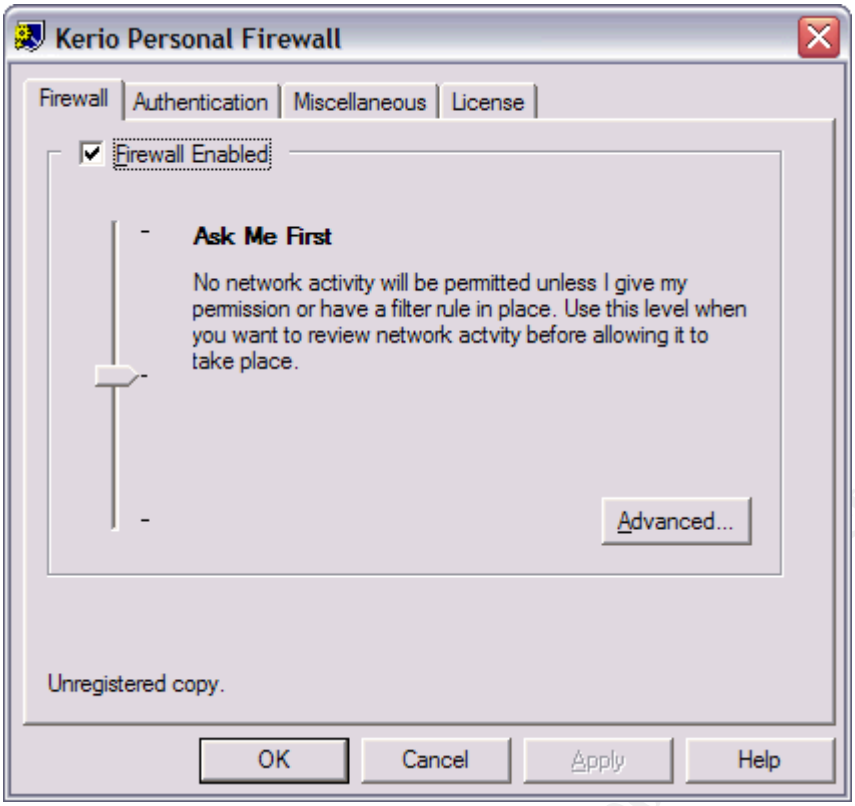
orientation. Check with the human resources department to see if time is available during these sessions where the organizations security policy may be explained verbally.

The face-time with the new employees helps them to understand what may be to them a very abstract science. Explaining many of the key issues in your organization and getting a discussion going with the new employees is time well spent. One way I have found that seems to both peak the new employees interest in InfoSec, as well as help the organization, is if you can frame your security "speech" toward the user at home. Information Security becomes personal when you explain to them how cookies work and that the session state may be captured while they are online with their bank. Explaining a SQL injection in terms of their credit card being stored at an online merchant can also get them thinking.

During the W32/Blasted and W32/Nachi worm infestation that hit the internet, we noticed that over 75% of the vectors of infection in our enterprise were from VPN and dial-up users coming into the organization on non-standard (or personal) equipment. While the employee is sitting at home on his children's desktop and dialing into the organization, your business is at risk. Explaining to the employee how when at home they can protect themselves by using personal firewalls and updated antivirus can assist you in keeping your network pristine; while the user is thankful his privacy is a bit safer.

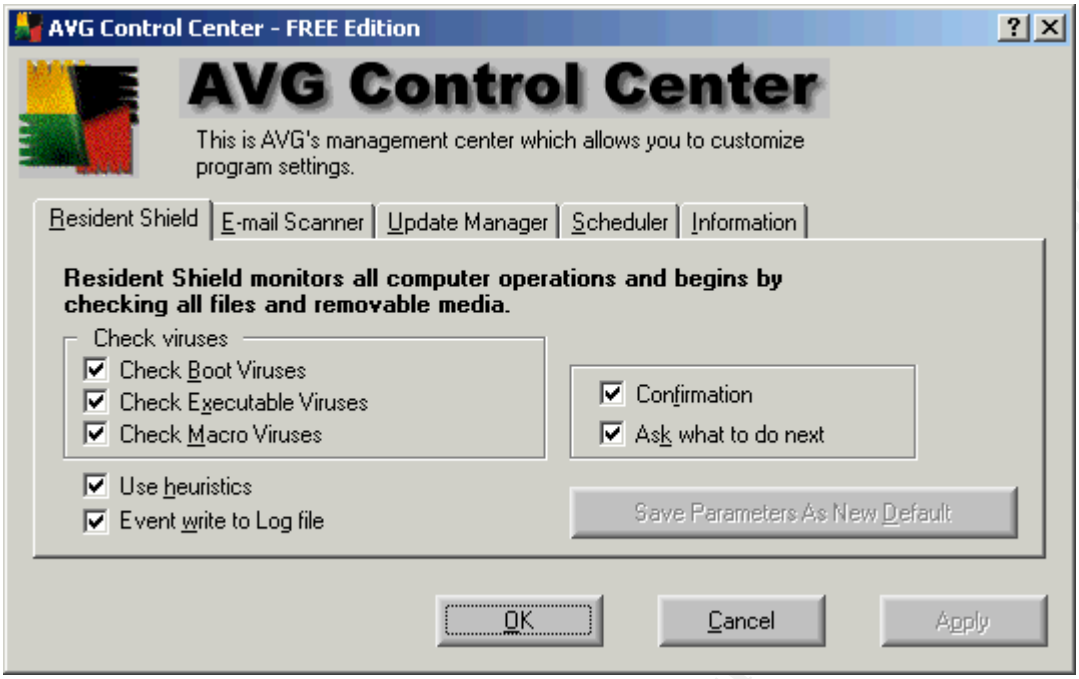
Below are a couple of examples of a free personal firewall software and an antivirus program that is available for your employees to use on their personal equipment for free.

PERSONAL FIREWALL



Above: Screenshot of Kerio Personal Firewall and its administration interface. Moving the bar to the top will block all communication. Sliding it to the bottom, will open all traffic. The current setting allows the user to configure the firewall rules on the fly as he will be prompted for what traffic to allow and deny. The Kerio Personal Firewall software is available at http://www.kerio.com.

ANTIVIRUS



Above: Screenshot of AVG Antivirus' Control Center interface. This interface is used to manage options within the software. AVG software is available at http://www.grisoft.com.

OH NO, NOT ANOTHER WINDOWS 2000 CHECKLIST

Finally, I have included as "Appendix A", a *Windows 2000 Server Minimal Baseline Security Checklist*; at least that is what I like to call it. As I mentioned above, the remote user accounted for a large percentage of worm traffic in recent months. Our second greatest threat were test and development servers that were stood up by developers who had little to no training in Windows 2000 server administration, let alone security. I approached a couple of the developers to enquire as to why their servers were configured so poorly when it came to installation of service packs, patching and general security. Their reply, to a man, was 'No one ever told us how to secure our servers'.

Well, under my keyboard I happened to have many scraps of paper I refer to for security configuration. I had written on everything from post-it notes to napkins. I decided it was time to codify this mess and pass it on for the greater good. I took a chance and emailed this document to our development and test shops so that someone would now have officially explained the "how" to them. The developers were extremely thankful to me for providing this to them. They now use this document in building their new servers, and we have helped mend a large hole in our network.

CONCLUSION

“Humans are usually the most susceptible point in any security scheme. A worker who is malicious, careless or unaware of an organizations information policy can compromise the best security” (Douglas E. Comer, Internetworking with TCP\IP Principles, Protocols and Architectures, 4th edition, Prentice Hall, 2000). There are many ways to save money in securing your IT architecture. Much of this can be done in lieu of spending funds on expensive software. This leaves funds available for your company to hire consultants to help teach your employees security awareness, and also purchase the needed items for which there may not be a free option. The best place to put information security dollars meant to protect the “CIA Triad” of **C**onfidentiality, **I**ntegrity and **A**vailability is to provide adequate user security awareness training.

Appendix A

Windows 2000 Server
Baseline Security Checklist for New Server Installs

A)

Permissions on the following drives\directories\files should be restricted (set permissions to only ADMINISTRATORS & SYSTEM; Full Control and AUTHENTICATED USERS "AU" the permissions as listed below):

There are issues with granting System Full Control. However, testing will have to be performed before limiting (SYTEM "FC" is the default).

Yes	No	C:	AU: Read & Execute
Yes	No	C:\boot.ini	
Yes	No	C:\ntdetect.com	
Yes	No	C:\ntldr	
Yes	No	C:\ntbootdd.sys	
Yes	No	C:\autoexec.bat	AU: Read & Execute
Yes	No	C:\config.sys	AU: Read & Execute
Yes	No	C:\Program Files\	AU: Read & Execute
Yes	No	C:\Winnt\	AU: Read & Execute
Yes	No	C:\Winnt\Config\	AU: List
Yes	No	C:\Winnt\Java\	AU: Read & Execute
Yes	No	C:\Winnt\Repair\	
Yes	No	C:\Winnt\Security\	AU: Read & Execute
Yes	No	C:\Winnt\System\	AU: Read & Execute
Yes	No	C:\Winnt\regedit.exe	
Yes	No	C:\Winnt\System32\	AU: Read & Execute
Yes	No	C:\Winnt\System32\Config\	
Yes	No	C:\Winnt\System32\Cacls.exe	
Yes	No	C:\Winnt\System32\regedt32.exe	
Yes	No	C:\Winnt\System32\rexec.exe	
Yes	No	C:\Winnt\System32\telnet.exe	
Yes	No	C:\Winnt\System32\tftp.exe	

"Everyone" group should be removed from all of the above when it appears. (See IIS section for possible exceptions.)

B)

Local Security Policy; Audit policy

- Set auditing to the following minimum :

Yes	No	Audit Account Logon Events	Success & Failure
Yes	No	Audit Account Management	Success & Failure
Yes	No	Audit Directory Service Access	Not Defined (DCs Only)
Yes	No	Audit Logon Events	Success & Failure
Yes	No	Audit Object Access	Failure
Yes	No	Audit Policy Change	Success & Failure
Yes	No	Audit Privilege Use	Success & Failure
Yes	No	Audit Process Tracking	Not Defined
Yes	No	Audit System Events	Failure

C)

- **Local Security Policy; Security Options**

Edit Default Settings to following parameters:

Yes	No	Additional Restrictions for Anonymous Connections	*No Access Without Explicit Permissions (DCs may be lower for compatibility with NT 4.0 systems)*
Yes	No	Clear Virtual Memory Pagefile When System Shuts Down	*Enabled*
Yes	No	Do Not Display Last User name in Logon Screen	*Enabled*
Yes	No	LAN Manager Authentication Level	*Send LM & NTLM-Use NTLMv2 session security if negotiated*
Yes	No	Number of Previous Logons to Cache	*0*
Yes	No	Restrict CD-ROM Access to Locally Logged-on User	*Enabled*
Yes	No	Restrict Floppy Drive Access to Locally Logged-on User	*Enabled*

D)

Missing MS Security patches

Yes No Install all patches on new machine using Windows Update utility until no critical updates remain. Will need several reboots and require multiple rescans of your box through Windows Update.

Be sure to include required Service Packs, roll-up patches and security patches for your OS, IIS, IE and any other apps. Also, make certain that you are running current versions of the software and not the original OS version (example: IE 5.01 installs with Windows 2000 Server; upgrade to IE 6.0 and apply IE 6.0 SPs and patches).

E)

Services Not Required

Stop and **Disable** the following services if they are running or if set to "Automatic" or "Manual" (if not specifically required by an application):

Yes	No	Alerter
Yes	No	Clipbook
Yes	No	Computer Browser
Yes	No	Fax Service

Yes No Indexing Service
Yes No Messenger
Yes No NetMeeting Remote Desktop Sharing
Yes No Print Spooler
Yes No Remote Procedure Call (RPC) Locator (Except on Domain Controllers)
Yes No Simple TCP/IP Services
Yes No Task Scheduler
Yes No Telnet

F)

Registry Lockdown

SYN floods

- Set the following parameters in the registry to further lockdown the server from SYN floods, etc. and protect the network:

Yes No Key:
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect
Type: REG_DWORD
Value: 2

Yes No Key:
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting
Type: REG_DWORD
Value: 1

Yes No Key:
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect
Type: REG_DWORD
Value: 0

Yes No Key:
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime
Type: REG_DWORD
Value: 300000

RDS Removal

- Remove the following keys if RDS is not required on the web server:

Yes No Key:
HKLM\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\RDSServer.DataFactory

Yes No Key:
HKLM\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\AdvancedDataFactory

OS/2 and POSIX Subsytem Key Removal

- Remove the following keys unless specifically needed.

Yes No HKLM\SOFTWARE\Microsoft\OS/2 Subsystem for NT
Delete all subkeys

Yes No HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment\Os2LibPath Delete

Yes No HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems\Optional Delete

Yes No HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems
Delete OS/2 and POSIX entries

- Verify no Write permission to HKLM\Software for all but administrator accounts.

Yes No Administrators & System: Full
Yes No Everyone: Read & Execute

G)

Internet Information Services

- Delete the following virtual directories in internet Services manager:

Yes No iisadmin
Yes No iissamples
Yes No msadc
Yes No iishelp
Yes No scripts
Yes No printers

- Remove default content:

Yes No C:\inetpub\wwwroot (and\or \ftproot and \smtproot)
Yes No C:\inetpub\scripts
Yes No C:\inetpub\iissamples
Yes No C:\inetpub\adminscripts
Yes No C:\program files\common files\system\msadc
Yes No %systemroot%\help\iishelp\iis
Yes No %systemroot%\web\printers
Yes No %systemroot%\system32\inetsrv\iisadmin
Yes No %systemroot%\system32\inetsrv\iisadmpwd

- Unmap the following extensions (unless specifically required):

(In order to unmap extensions, in ISM go to "Home Directory" tab and choose the "Configuration" button.)

Yes No .asa
Yes No .asp

Yes No .bat
Yes No .cdx
Yes No .cer
Yes No .htr
Yes No .htw
Yes No .ida
Yes No .idc
Yes No .idq
Yes No .printer
Yes No .shtm
Yes No .shtml
Yes No .stm

- Disable all unnecessary ISAPI filters (Do this under ISM, ISAPI filters tab).

Yes No Delete the Frontpage ISAPI filter (or extensions on older IIS servers), if you have a choice. If Fronthpage ISAPI extensions are required, make them READ ONLY. On older IIS servers, disable Frontpage extensions with the following command "C:\program files\common files\microsoft shared\web server extensions\40\bin\fpsrvadm – o uninstall –p all".

Yes No Delete the Digest Authentication filter. This authentication method requires support for reversibly encrypted passwords—which is a very bad idea.

Yes No Delete HTTP compression filter. This filter allows compression of the HTTP stream. Although a nice feature, there are security related implications. This should be considered a "Low" at this juncture.

- Disable "Enable Parent Paths" setting.

  Yes No In ISM, go to "Home Directory" tab, "Configuration", "App Options" tab and uncheck the applicable checkbox.

  (This prevents malicious web folder\directory traversal without knowing the underlying directory structure. Web developers can not use paths such as ..\..\default.htm and must use fully qualified paths.)

- Default websites should not be on the system drive.

  Yes No Move sites to separate partition.

- Minimum permissions needed should be set:

  Yes No NTFS: Read
  Yes No IIS: Execute.

  IIS: Read is NOT required and will allow a cracker to download your code.

  Web applications (i.e., scripts and executables) only need a limited amount of permissions to run properly. Giving more permissions than is necessary allows a malicious user to download and analyze your code for vulnerabilities.

- Set permissions to IIS logs to:

  Yes No System and Administrators group only

- Restrict NTFS permissions to ALL executables on system. NTFS perms:

  Yes No Administrator & System: Full
  Yes No Users: Read & Execute

  Give the IUSR account the execute permission sparingly.

- Restrict permissions to any script interpreters such as PERL. NTFS perms:

  Yes No Administrators & System: Full
  Yes No Everyone: Read & Execute

  Give the IUSR account the execute permission sparingly.

- No PERL interpreters in default directories.

  Yes No Interpreters and Shells are in separate folder\directory from scripts.

- If necessary, add and/or check permissions to ensure "Everyone" group has a maximum of "Read Only" on (only if necessary):

  Yes No %webroot%
  Yes No %sytemroot%
  Yes No %systemroot%\system32
  Yes No %systemroot%\system32\inetsrv
  Yes No %systemroot%\system32\inetsrv\asp
  Yes No %systemroot%\program files\common files\

H)

Anti-Virus Settings

NetShield AV Scan Engine:

Yes No Update scan engine to, minimally, 4.2.60.

All other attributes of AV seem to be configured properly.

Yes No Heuristics are enabled and scans are of all files.
Yes No Weekly scan is enabled.
Yes No Automatic updates set to run daily.
Yes No On Access scans are set to run on ALL files.

I)

Rename Accounts

Yes No Rename Administrator account to "webroot" (or a different admin account naming policy that your group may use).

Yes No Rename Guest account to "nomoreguest". (Or other account name. Also, verify account has not been enabled).

My own suggestion is: Rename "administrator" as suggested above to "webroot". Rename "guest" to "administrator".

J)

Configure Explorer To Show File Extensions

(This helps prevent you from running dangerous programs that you might have downloaded by mistake, such as Registry files or .VBS files.)

Yes No Go to Windows Explorer -> Tools -> Folder Options -> View

Un-click "Hide file extensions for known file types".

Select "Show hidden files and folders"

Select the button called "Like Current Folder" to put these preferences in all directories/subdirectories.

This will prevent you running the file you downloaded that you think is called "ourfamily.jpg" (or "dancingpigs.jpg" or whatever you are into) but is really a trojan named "ourfamily.jpg.exe" which will infect your system and then others.

K)

Disable Guest Access to Log Files

Yes No Disable guest access to Application Log:

Key:
HKLM/System/CurrentControlSet/Services/EventLog/Application/RestrictGuestAccess
Type: REG_DWORD
Value: 1

Yes No Disable guest access to Security Log by adding:

Key:
HKLM/System/CurrentControlSet/Services/EventLog/Security/RestrictGuestAccess
Type: REG_DWORD
Value: 1

Yes No Disable guest access to System Log by adding:

Key: HKLM/System/CurrentControlSet/Services/EventLog/System/RestrictGuestAccess
Type: REG_DWORD
Value: 1