

Consensus Minimum Security Benchmarks

A Gold Standard for Windows 2000 Professional Arises from a Public-Private Partnership

by Alan Paller, SANS Institute; and Clint Kreitner, The Center for Internet Security

The Gartner Group reported last May that at least through 2005, 90 percent of computer attacks will use known security flaws for which a solution is available. People don't fix the flaws because—

- knowledge about the flaws and how to fix them is not widely shared, and
- tools to measure whether they have been fixed were not widely available”

On July 17, the National Security Agency, Defense Information Systems Agency, the National Institute of Standards and Technology (NIST), the FBI's National Infrastructure Protection Center, the General Services Administration (GSA), the SANS Institute, and the Center for Internet Security (CIS) jointly announced minimum standards for securing computers using Microsoft Windows 2000 Professional, which is used on Windows 2000 computers functioning as workstations. The unprecedented announcement, led by Presidential Cyber Security Advisor Richard Clarke, is an effort to stop most common attacks against computer networks both inside and outside the Government. The new benchmark provides detailed configuration specifications for computers running Windows 2000 Professional and that are to be connected to networks. In field tests, application of the benchmark configurations have proven to eliminate more than 80 percent of commonly exploited vulnerabilities. (see *Measuring the Value of Security Guides* on page 10 for details on the effectiveness of the new benchmarks).

Government experts hope that the benchmarks will help eliminate two of the most troubling problems in computer security—problems that affect both federal and private computer networks—by eliminating holes that hackers already know about.

Two widespread problems

Unprotected systems are a massive challenge throughout Government and industry because of two practices common among companies that sell and install systems.

First, the companies employ a distribution process in which months pass between the time a vendor creates a CD and a user installs the software. Even if you are the first to receive a new CD, the software on that CD may be two or three months old. Security vulnerabilities discovered in the intervening months are automatically installed with the software. Users may overcome this problem by downloading and installing the latest security patches from the vendor's Web site, but, not surprisingly, a large percentage of users do not take this step.

While the systems remain unpatched, they are highly vulnerable. More than two thousand automated attack programs are constantly scanning the Internet looking for vulnerable systems. Too many organizations have found that their systems are attacked and exploited (often with a Trojan horse program) before the users have had time to download and install the needed patches.

Second, the companies deliver their software with installation scripts that automatically install services that are unfamiliar to the user and may not be needed. Some of those services, like telnet, FTP, CGI scripts, and BIND/DNS are notoriously vulnerable to attackers. Others have more subtle vulnerabilities. All of them, if left enabled, provide a continuing fertile ground for additional vulnerabilities to be discovered and exploited. When users do not know they are running a service, they often do not look for security patches for those services.

The White House announces a standard for DoD and possibly other agencies

In announcing the new benchmark, President Bush's Special Advisor of Cyberspace Security, Richard A. Clarke, pointed out the most important aspect of the new benchmark, saying, “this is the model for Government and industry partnership.” The partnership combines the knowledge and buying power of the Government and more than 100 very large non-Government organizations. They agreed on specific minimum security settings for Windows 2000 Professional presented as a “gold standard.” Mr. Clarke also said that DoD organizations would be required to use the new standards and that the White

House is considering whether and how to require compliance by civilian federal agencies.

Consensus takes some of the uncertainty out of security

Most of the organizations involved in the partnership had published their own guides for securing Windows 2000, but all the guides conflicted in small ways. Since many user organizations looked to multiple sources for guidance, the differences between their guides meant that they were unable to move ahead with confidence.

The consensus benchmarks were forged by all the organizations identifying and resolving the differences among the various existing guides. The consensus guide empowers user organizations to move ahead with a high degree of confidence that they can have a solid foundation for security of their systems.

Tools to test and enforce the standards

As a part of the announcement, the partners also released an automated testing tool created by CIS that compares the security settings on a computer with the security settings in the benchmark and scores each machine on a 0 to 10 scale.

Benchmarks are complex documents and most system administrators and security practitioners have neither the time nor the breadth of expertise to test every aspect manually. Automated testing makes that job easy and reliable. The Center's tool also guides the user in the proper method of correcting configuration problems that lower the score.

U.S. Air Force plans to acquire safer systems

At the July 17 announcement, U.S. Air Force CIO John Gilligan announced that the U.S. Air Force was planning to integrate the new benchmarks into future procurements so that system administrators would not be burdened with having to play catch up on every new machine.

Where to find benchmarks and tools

The benchmarks and automated tools are available for immediate download from the CIS's Web site at <http://www.cisecurity.org>. Individuals may use the benchmarks and tools to check their systems, but organizations must be members of the Center to distribute the tools and use them across the entire organization. The GSA has purchased internal distribution rights for all Federal Government agencies (both civilian and Military), as well as for authorized federal contractors and sub-contractors, so that they may use the tools wherever and however they see fit on Government

...continued on page 9

Additional Benchmarks Currently Available from CIS

<http://www.cisecurity.org>

- **Cisco IOS Router**—The most popular router
- **Solaris**—The UNIX operating system used on Sun Microsystems computers
- **Linux**—The open source operating system gaining popularity in government and industry
- **HP-UX**—The UNIX operating system used on Hewlett Packard computers
- **Windows NT**—The most popular server operating system on Intel hardware prior to Windows 2000.

Training and Certification for Implementing the Windows Security Benchmark

The new security benchmarks will improve security only on the systems where they are applied. The ultimate value of the benchmarks, therefore, will be determined by the number of people who have the skills and knowledge to implement them.

Because that knowledge is not taught in Microsoft system administration courses for MCSA or MCSE certification, security experts from Australia to the U.S. to Europe have cooperated to build a hands-on education program that targets the necessary skills.

The course covers the benchmark, what it does, including registry keys, folder ACLs, user rights, and security policies. It also shows how to view, modify, and apply the standard. And the course provides hands-on experience in using the tools that enable administrators to be sure it is being applied correctly. It assumes the student is familiar with Windows 2000.

To reach a goal of training 150,000 people in applying the security benchmarks, five types of education have been deployed—

1. The course book is available from Amazon and is called "Securing Windows 2000 Professional Using the Gold Standard Security Template" by Bower, Farrington, and Weber, (ISBN 0-9724273-0-9).
2. Hands-on, instructor-led training has been run in more than 50 cities around the world both in public courses and in private onsite courses.
3. On-line training is available at any time with audio programs, visuals, and on-line quizzes.
4. Local-mentor programs are also being launched in more than 60 cities and on military installations. These programs combine on-line training with two or three meetings in which mentors help their peers work through the hands-on exercises.
5. Instructor-led on-line training is also being offered in which students take the live course with an instructor, but do so remotely.

Certification Program

Each student may demonstrate that both skills and knowledge have been mastered by completing a practical exercise and passing a test.

For information on the availability of DoD education programs for the new benchmarks, contact DISA, Maryann Dennehy at 703/882-1716. For more information on training programs open to all students, see the schedule posted at <http://www.sans.org>.

Training System Administrators in Using the New benchmarks

- **AIX**—The UNIX operating system used on IBM computers
- **Apache Web Server**—The most popular Web server software
- **Windows IIS Web Server**—The second most popular Web server software
- **Check Point FW-1/VPN-1**—The most popular firewall/VPN
- **Cisco PIX Firewall**—The second most popular firewall
- **Cisco CAT Switches**—The most popular networking switch



The Importance of Consensus Security

by Tony Sager and Brian Henderson

IAnewsletter

Volume 5 Number 3 • Fall 2002

<http://iac.dtic.mil/iatac>

The Department of Defense (DoD) and many other components of the Federal Government look to the National Security Agency (NSA) for the means to protect vital communications and information systems. In today's Information Technology environment, the need is particularly acute for ways to counter security vulnerabilities found in popular commercial operating systems and applications. The NSA's Information Assurance Directorate (IAD) has responded to the challenge, in part by developing a very successful series of Security Configuration Recommendation Guides. And, in a real break from tradition, several of these Guides have been shared with the public through the NSA Web site <http://www.nsa.gov>. On July 17, 2002 at the press conference led by Richard Clarke, Cyber Security Advisor to the President, we joined with a number of our peer organizations to announce agreement on a "consensus" security benchmark for Windows 2000.

Several customers who had adopted our earlier NSA *Microsoft Windows 2000 Security Recommendation Guides* wanted to know if we had changed course. We reassured them that the content of the consensus benchmark is essentially identical to our prior NSA Guides. Here's the message that we asked them to take away from the press conference. This is a change in the development process for this type of security guidance, and that our goal is to reach agreement on baseline security configurations among peer organizations (the Defense Information Systems Agency [DISA], the National Institute of Standards and Technology [NIST], the FBI's National Infrastructure Protection Center, the General Services Administration [GSA], the SANS Institute, and the Center for Internet Security [CIS], etc.).

A shared problem

Why did we move towards a "consensus" model for developing and sharing security recommendations?

Fundamentally, it is because we believe that, at the security baseline level, network security is a shared problem between the DoD and the rest of the community. Not only is our security problem shared, but also we are each hope-

lessly dependent upon the security of others. If we have a shared problem, then we must pursue shared solutions.

There had already been a lot of technical sharing between several organizations that develop such standards (NSA, DISA, NIST, CIS, etc.). Here's the challenge we set before ourselves—if we could come to agreement on a common baseline, then the community would benefit in several ways. We could share labor on the development and the maintenance of security guidance. As the community following the guidance grows, "spin-offs" like training and tools become more viable for vendors to provide. Most importantly, we could minimize the confusion for system operators, who are already flooded with multiple authoritative sources and conflicting security guidance.

So this change in focus and attitude led to a surprising result—community agreement among a large number of security experts on prudent, baseline security settings for Windows 2000.

Consensus is nice, security improvement is better

But here's the reality check.

No security guidance document, however well intentionally and thoroughly tested, is inherently "good." Security guidance is only valuable when used and when it becomes a routine part of designing, installing, and operating our networks. This means that it must be easily integrated into operations, supported with tools and training, and provide a clear implementation of site and higher-level security policies, all in addition to providing specific value in improving security.

The bottom line? Security benchmarks are not the final answer for security improvement—they're just a beginning. Real improvement in network protection will come in many forms.



Benchmarks

1 When system owners and decision makers move to adopt this consensus guidance for operational networks.

We're not starting from scratch. Each of the organizations involved in the consensus brings along a very large constituency. For NSA's part, we know that hundreds of organizations and major programs all across Government and the private sector have already adopted our guidance, formally as we support them through our mission, and informally by taking our recommendations from the Web site.

On July 17, U.S. Air Force CIO John Gilligan announced his intention to make the Windows 2000 Consensus Benchmarks the U.S. Air Force standard. The earlier NSA Guide, with essentially identical content, was declared the DoD Baseline Standard for Windows 2000. A number of other organizations are considering similar large-scale adoption.

If you follow security guidance for Windows 2000 available from DISA, NSA, NIST, CIS, or SANS, then you are already part of this consensus movement. The key difference is that the people giving you advice have agreed to share their ideas up-front, and reach agreement wherever possible.

2 When security engineers routinely start from and adapt consensus security benchmarks for their customers.

We know this is starting to happen across the community. MITRE system engineers supporting DoD (some of whom are directly involved in the development of the guidance) now routinely use the consensus benchmarks (or its predecessors like the NSA Recommendation Guides) as a starting point for advice to DoD programs. Anecdotally, we have heard numerous stories of use of the benchmarks from Microsoft senior engineers—using them as a starting point, and tailoring them to the specific operational and security needs of their customers.

3 When the consensus security benchmarks are supported with training.

SANS quickly had a course available based on the consensus benchmarks (their "Gold Standard" training), which is selling out rapidly. DISA is developing training based on

this technical content, and the DIAP is exploring options for DoD-wide training. Large-scale, reasonably priced training from commercial sources integrated into Military schools is easily within reach.

4 When the consensus security benchmarks are supported by tools to help manage networks.

Consensus security benchmarks will not improve the security of networks on a large scale until they are embodied in a rich selection of tools to assist system administrators. Tools allow a system administrator to implement the benchmarks, and enable periodic or continuous reporting on the actual settings of every machine. The effect of configuration changes, and the resulting security improvement, can be scored, measured, and reported. This view of security status can then be used as the basis for enterprise level security metrics.

A fundamental part of the CIS model is the development and release of freeware tools that measure compliance with their benchmarks (and with the consensus). But their real goal is to encourage a large market for commercial tool builders by certifying vendors whose tools accurately report on compliance with benchmarks. Based on technology that they already offer, commercial tool vendors can easily build compliance checkers that measure systems against these best practices. The vendor enthusiasm seems very high, and vendors like Bindview, Symantec, and NetIQ have already committed to this.

5 When consensus security benchmarks are available for each of the key components found in our networks.

A security benchmark for Windows 2000 is just the beginning. Most of the technical work is already done for Solaris and Cisco IOS, and these will be available and supported by CIS tools very soon. Several others are underway. Our mutual goal is to continue the consensus model, and share work wherever possible. This work can move quickly because organizations like NSA, DISA, and CIS are contributing existing documents as a "first draft" for the community.

6 When we can change our security decision processes.

With a defined baseline we can change how we purchase, deliver, and test software. If we think of the consensus security benchmarks as specifying the desired security behavior of a system and its applications, we can then provide a standard test environment for GOTS developers, and acceptance criteria for applications.

Key security decisions like accreditation, certification, and network “readiness” can become much more streamlined and meaningful. If we think of the benchmarks as representing the “best advice” of the security community, then—

- System architecture and design could start from such benchmarks for each component
- Security engineers could tailor the benchmarks based on program-specific security issues and operational constraints
- Documentation of the security-operational trade-offs could serve as key evidence to decision makers about the security worthiness of the resulting system
- Continuous measurement of the tailored security benchmarks with tools can provide decision makers with a meaningful metric of the “readiness” of the network

Security “value”

Given the track record of the organizations involved, many people accept that the consensus security benchmarks for Windows 2000 are worthy of attention, if not adoption. However, we think that analytic organizations (including ours) owe the operational community and senior decision makers a clearer and more specific case for the potential security value of moving towards consensus benchmarks as a model for operating our networks. These are some of the questions that the operational community should pose about the potential security value of consensus security benchmarks—this is the sort of discussion that can get mired in philosophical debate and misleading statements (e.g., “this will stop 90 percent of all hacker attacks”).

1 Do they “close” most of the known vulnerabilities in the component?

There’s no final answer, but current informal studies, using different techniques for measurement, show that compliance with the consensus security benchmarks for Windows 2000 Professional (or predecessors like the NSA Guides) will conservatively close well over 80 percent of the known vulnerabilities in that component (see the feature article *Consensus Minimum Security Benchmarks: A Gold Standard for Windows 2000 Professional Arises From A Public-Private Partnership* on page 4). More detailed studies are underway at MITRE and elsewhere, including the mapping of common vulnerabilities and exposures (CVE) vulnerabilities against the benchmarks (see *Enterprise Security Enabled by CVE®* on page 12).

2 Do they “block” attacks against our systems?

Organizations that have collected and/or analyzed data about attacks against systems (e.g., the DoD CERT, CERT/CC, Gartner Group) all use very similar numbers—90 percent or more of the attacks or incidents against systems have taken advantage of known vulnerabilities with known solutions (e.g., patches or configuration options). In fact, it is typically reported that most attacks are based on a relatively small number of specific vulnerabilities. This is an area that deserves more study, and we believe that these two complementary communities—organizations that track, analyze, and report on attacks, and organizations that analyze technology and develop security recommendations—should jointly take this as their challenge.

3 Do they help me manage vulnerability information, by filtering through the “security noise” and helping me respond to new vulnerabilities?

The operational community does not have the luxury of time or resources to turn every system administrator into a security “wizard.” If, in fact, compliance with consensus security benchmarks will close most vulnerabilities and block most attacks, then system operators can spend much less time sorting through the “security noise” of multiple vulnerability alerts, conflicting experts, and vendor claims. The effort of developing the consensus security benchmarks brings together security experts in both the public and private sectors to study vulnerabilities, develop countermeasures, and share the information in a form usable by system operators. As new vulnerabilities are uncovered, these experts should be able to quickly assess the effectiveness of prior guidance, and update it if necessary.

If compliance with the consensus security benchmarks will close most vulnerabilities and block most attacks, does this imply that the “consensus” organizations have discovered some magic ideas that everyone else missed? Of course not. In fact, our experience shows that qualified, independent groups (including the vendor) that develop security configurations for a component will typically reach very similar conclusions. This is not surprising, since all of us are studying the same “pile” of vulnerabilities, and the options for blocking problems at a component configuration level are relatively limited.

Therefore, the unique aspect of the security benchmark for Windows 2000 is the level of agreement among organizations, not the specific content of the benchmark. The benchmarks provide a vehicle to focus the experts, gain feedback from the operational community, and translate the hard-earned knowledge of vulnerabilities into a constructive, usable form that can improve security. In this way, everyone can spend less time sorting through the noisy pile of vulnerabilities, and more time on missions and operations.

No benchmark or guide will solve all security problems

Here are a couple of things that skeptical readers should point out about community-wide security benchmarks. There are no “magic bullet” solutions to the network security problem. For the Windows 2000 example, at best we can speak of closing almost all of the known vulnerabilities for only one component in a potentially very complex system.

However, it is a very significant subset of the applicable vulnerabilities for a key component of the network and, as discussed above, seems to easily meet the “80 percent solution” threshold. Given the state of network security today, an approach that can make much of the vulnerability management problem tractable and is “reasonable” in cost, training, implementation, and maintenance is an essential step.

Security is a system level problem, but we believe that without strong, known building blocks, system security is unattainable.

Benchmarks are not the long term solution

Gaining agreement among security experts and system operators is essential, gratifying, and has the potential to bring about large-scale security improvement. However, this strategy is essentially reactive—blocking problems after they are discovered, and doing the best that we can with existing technology. This approach is not the long-term solution.

However, benchmarks can be used to “attack” the security configuration problem earlier in the life cycle. They can be used to specify how systems are configured out of the box, or delivered by our systems integrators. They can provide a testing baseline for applications developers, and as a means to collect community agreement on expected system behavior for the product developer. We are also developing closer linkage to the National Information Assurance Partnership (NIAP), to ensure that the development of more secure systems is closely matched to the secure operation of systems.

Summary

In our experience, the working-level cooperation between Government Agencies, private companies, and Microsoft that led to the success of the security benchmark for Windows 2000 is unprecedented, and the feedback has been overwhelmingly positive. The most gratifying feedback is from system administrators—the people on the front lines who have to make the technology work, and who rely on the security community for their help in securing systems.

The people involved in this project are representative of a growing security community, an extended network of professionals in and out of Government who have dedicated their careers to improving the security of our nation’s information and networks. Our collective sense of purpose has never been more focused, and the spirit of cooperation has never been higher. Working in partnership, we have the ability and the responsibility to improve the security of our nation’s information systems. ■

About the Authors

Tony Sager

Tony Sager serves as the Chief of the Systems and Network Attack Center (SNAC), located in the Information Assurance Directorate of NSA. The Center develops and releases to the public the NSA Security Recommendation Guides for several IT products (Windows 2000, Cisco Routers, etc.). Their security analysis of emerging network technology is sought and used by policy makers, network architects, and users across government. Tony recently celebrated 25 years with the NSA, holding a number of technical and managerial positions focused on Computer and Network Security. He holds a B.A. in Mathematics from Western Maryland College and an M.S. in Computer Science from the Johns Hopkins University.

Brian Henderson

Brian Henderson has been involved in information assurance since 1985. As a U.S. Naval officer and a graduate from the Naval Postgraduate School, he was assigned to the Department of Defense (DoD) Computer Security Center at the NSA. Following retirement from the U.S. Navy, Mr. Henderson worked for a small software support firm developing support plans for DoD information assurance products. He joined NSA in 1998 developing information assurance policy, then served on the NSA Chief Information Officer’s staff. Mr. Henderson joined the SNAC in 2001 as Chief of Staff and helped coordinate the center’s efforts to make security configuration guidance available to the public. He is currently a full-time student at the DoD Joint Military Intelligence College pursuing a Master of Science degree in Strategic Intelligence.

...continued from page 5

owned computers and contractor computers being used for Government tasks.

The bottom line

Turning the tide against cyber attackers will not be possible until the vast majority of systems on the Internet are free of common, easy-to-exploit vulnerabilities. The Gold Standard consensus benchmarks offer a means to accomplish that goal on both newly acquired systems and on systems already deployed.

The consensus benchmark process does not guarantee security—no one and no single action can. Rather they raise the bar for would-be hackers and crackers and dramatically reduce the vulnerability of all who apply the benchmarks and measure their systems, and all who connect to the them. ■

About the Authors

Alan Paller

Alan Paller is Director of Research at the SANS Institute. He leads SANS consensus research programs, was the expert witness in the MafiaBoy trial, has testified before both the House and Senate, and has chaired more than 60 national and international conferences on information technology. He may be reached at paller@sans.org.

Clint Kreitner

After serving in the U.S. Navy as Director of Computer-Aided Ship Design at the Bureau of Ships and Design Superintendent, Clint Kreitner has for the past 30 years been President and CEO of two information technology companies; ROH, Inc. and American Information Systems, Inc. (1971–1989); and numerous hospitals (1989–2000). Most recently he was President and CEO of the Southeastern Region of the Adventist Health System. He served as a Board Member and was Chairman of the Board of several of the hospitals. He is currently the President and CEO of The Center for Internet Security. Mr. Kreitner earned an undergraduate degree from the U.S. Naval Academy and graduate degrees from Webb Institute and American University.

Measuring the Value of Security Guides

security
vulnerabilities

by Trent Pitsenbarger

Why should I implement these security recommendations? What benefits do they provide? How much will they improve the security of my systems? These are the pervasive questions that we have been asked since we published our first security guide in 1997.

Historically, one of the primary missions of the NSA's Systems and Network Attack Center (SNAC) has entailed the provision of security consultancy services to the Department of Defense (DoD) and U.S. Government Agencies. These services have run the gamut from architectural guidance provided at the onset of network design to field evaluations of fully operational networks.

In the mid 1990s, demand for these services increased dramatically in response to the growing dependency of our customers on information technology (IT). Realizing that customer demand was beginning to outstrip our capacity, the SNAC began development of a series of security configuration documents that system administrators could use to help secure their networks. The goal was to offer the benefit of our knowledge and experience via the guides with the primary audience being those customers with which we could not directly interface. In 1997 the SNAC delivered its initial set of guides, covering Windows NT, Microsoft Exchange, and Lotus Notes.

From these rather humble beginnings the suite of configuration guides has grown dramatically. Presently 34 guides are available on the NSA Web site, covering a wide range of topics. The Web site is in its 17th month of operation and is currently enjoying over 1,000 unique visitors per day with over 2 million total downloads. The guides are used by a plethora of customers, are endorsed by the vendors whose products they cover, have formed the basis of commercially available tools used to assess and improve the security posture of networks, and have been endorsed by a variety of private sector security forums and key industry personnel. Most recently, these guides formed the basis for the development of the Windows 2000 Professional Consensus Baseline Security Settings.

Intuitively, these guides have been a remarkable success and while these are all strong indicators that the guides have been beneficial, is there a more quantifiable means

of determining the value of these guides? The SNAC has postulated several methods of measuring value. One of the simplest, and most meaningful entails "before and after" vulnerability scans. In other words, what reduction in vulnerabilities is reported by vulnerability scans as a result of the application of the security guidelines?

In order to develop such hard and fast numbers, the SNAC utilized a popular commercial vulnerability scanner. This scanner monitors a computer under evaluation and reports on over 2000 known vulnerabilities, which it categorizes as being of high, medium, or low concern. The scanner reports on internal configuration settings, file and registry permissions, policy issues, and application level vulnerabilities. For our testing, the vulnerability scanner was run against an out-of-the-box configuration of Windows 2000 Professional and was then re-run after implementing the Windows 2000 Baseline Security Settings. As recommended in the guidelines, implementation of the settings included the installation of Windows 2000 Service Pack 3 and the cumulative patches for Internet Explorer and Windows Media Player. The implementation of these patches is critical. While the overall network architecture and configuration of a computer can, in some cases, mitigate problems addressed by security patches, there are many instances where the only practical countermeasure is to install the patch.

As a result of implementing the Windows 2000 Baseline Security settings and applicable security patches, the number of vulnerabilities in the "high" category dropped 95.5 percent while the overall number of vulnerabilities dropped 90.7 percent! Figure 1 illustrates the complete set of results from these tests.

In a related effort, the MITRE Corporation performed their own independent analysis of the value of the guides. The goal of this analysis was to identify the number of common vulnerabilities and exposures (CVE) issues present in various configurations of Windows 2000 Professional (see *Enterprise Security Enabled by CVE®* on page 12 for more information). The end result was that with Windows 2000 Service Pack 2 installed, post SP2 hot fixes installed,

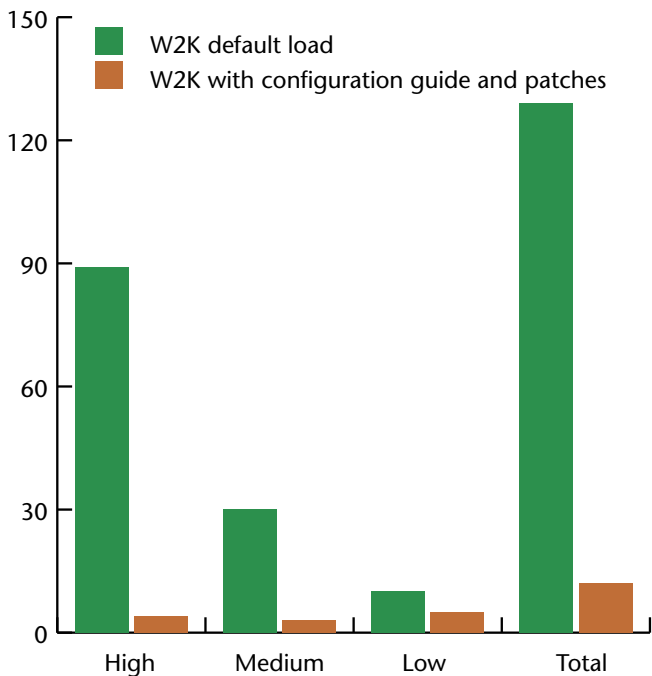


Figure 1. Windows 2000 vulnerability scanner results

and the consensus baseline settings applied, 83 percent of the CVE vulnerabilities were eliminated.

In both of the above studies, the figures were derived from analysis of systems within laboratory environments where operational considerations were not a limiting factor for implementing the security guides. However, it is important to note that similar results have been demonstrated based on the configuration and analysis of operational systems. A case study documenting these results is available from the Center for Internet Security's Web page <http://www.cisecurity.org>.

So what about the residual vulnerabilities not covered by patches and the Consensus Baseline settings? Several of these residual vulnerabilities are related to optional configuration settings that can be applied in high-risk environments when operationally feasible. However, most of the residual vulnerabilities are related to application level settings not covered by the operating system configuration

guide. Implementing other configuration guides, such as the various SNAC application guides, would have reduced the vulnerability space even more.

To demonstrate this, similar tests were performed using Microsoft's Internet Information Server (IIS) software and the corresponding SNAC IIS guide. The vulnerability scanner that we utilized tests for a variety of configuration issues as well as checking the patch status of the IIS installation. Our testing showed that 50 percent of the vulnerabilities identified by the scanner were corrected by the application of the configuration settings alone, with all of the vulnerabilities addressed when both the guide and security patches were applied. These numbers reflect the nature of IIS security patches—they tend to be related to port 80 based buffer overflows against which IIS configuration settings are generally ineffective.

These numbers are impressive but we do not mean to imply that this is a "magic bullet" solution to network security. Proper configuration of the operating system and applications along with timely installation of security patches are just two elements of a sound and comprehensive security policy, but if followed universally would significantly raise the security posture of our networks. ■

References

1. The Windows 2000 Professional Consensus Baseline Security Settings can be found at <http://www.cisecurity.org>.
2. All the SNAC guides can be found at <http://www.nsa.gov/snac/index.html>.

About the Author

Trent Pitsenbarger

Trent Pitsenbarger has worked at the NSA for 18 years. For the last six years, he has worked as a technical leader in NSA's SNAC. In this role, he provides computer security consulting services to a wide variety of civilian and military organizations. He has a M.S. degree in Computer Science from James Madison University. He has authored numerous security configuration guides which have been published to the NSA's Internet Web site.