Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Best Computer Security Practices for Home, Home Office, Small Business, and Telecommuters

In this paper, the author recommends utilizing a multi-layered defense security approach to secure home, home office, small office, and telecommuter computers.

Copyright SANS Institute
Author Retains Full Rights

AD

Best Computer Security Practices
for Home, Home Office, Small Business, and Telecommuters
Jon Willert
October 22, 2001

Introduction

Nimda, SirCam, CodeRed, SubSeven and dozens of other backdoors, Kak, SpyWare, DDos attacks affecting even the largest of web sites, Social Engineering, default operating system security holes, and application security holes, and many others should cause a wide range of emotional reaction to over 94 million people who use the Internet at home[1]. Unfortunately, for all of us, it does not necessarily mean that they are proactively managing their computers. This only makes the Internet and Computer Security for those who do proactively manage their computers and computer networks more critical and less secure. There is a balancing act to balance computer security with usability but it is becoming more important that everyone become more secure.

"Most of the security tips you find these days will slow down a determined hacker - for about 5 seconds. By that time, his highly modified script has blasted past the errors you've fixed in your operating system and finds the one hole you left unplugged."[2] "We all know that two-thirds of corporate hacks come from inside the firewall, making internal security as important as external. But what about your remote offices and SOHO workers? Are they as vulnerable to attacks as your corporate workers? Yes. Definitely."[3]

I am recommending the following best practices utilizing layered security to secure home, home office, small office, and telecommuter computers.

"Why layered? Nearly two-thirds of all security breaches are caused by insiders accessing unauthorized information - something a corporate firewall can't stop. Most security experts believe layered security is the way to go, as it's only a matter of time before someone finds their way through any single layer. Furthermore, a good layered security system not only protects your key network access points, but also protects them against different avenues of attack, known as vectors, including insider attacks."[4] Additionally, if any one of your layers has or develops a security weakness or is incorrectly configured, hopefully the other layers can and will still provide sufficient protection from the majority of the attempts. This layering method for computer security protection will also lessen the criticality of selecting the best of each layer; **it is more important to have the layers than it is to have the best at each layer!**

---

[1] http://www.census.gov/prod/2001pubs/p23-207.pdf
[2] Janss, http://www.nwfusion.com/reviews/2000/0807rev.html
[3] Janss, http://www.nwfusion.com/net.worker/news/2001/0806networkerreview.html
[4] Janss, http://www.nwfusion.com/net.worker/news/2001/0806networkerreview.html

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

1 - Utilize current antivirus software, properly configure it, and update it accordingly*

2 - Utilize a software-based personal firewall, properly configure it, and update it accordingly**

3 - Utilize a router/firewall device for your Internet connection, properly configure it, and update it accordingly (whether it is dial-up, DSL, cable modem, or other)

4 - Update your operating system with security updates

5 - Update your applications with security patches

6 - Update your skills and knowledge, constantly

*If you use the Internet occasionally (one hour per day or less), update your antivirus software weekly. If you use your Internet daily (one hour per day), update your antivirus software daily. If you use your Internet extensively (more than one hour per day), or are involved with computer security, update your antivirus software hourly (if possible, as Norton Antivirus allows). I suggest changing the real-time and manual scans to scan ALL files. The overhead in performance seems worth it compared to lost, deleted, or corrupted data and the time-consuming process to rebuild a system and make it functional gain. These suggestions may seem extreme, however, the frequency of the updates are based on my experience with thousands of servers and workstations and their unfortunate and often untimely infection from various computer virus and other malware. Some people may also consider this paranoid, however with hundreds of new computer viruses found every month and with the rate of transmission and infection, antivirus software must be updated often to be effective.

**If your personal firewall is from the same vendor as your antivirus software, update the personal firewall at the same frequency as the antivirus software. If your personal firewall is from a different vendor, update it weekly.

Background

I have been researching, installing, configuring, and testing computer security solutions for about 15 years. Some of the security solutions and firewalls include Novell BorderManager, Axent Raptor, NAI Gauntlet, Checkpoint, Microsoft Proxy Server, Microsoft ISA, Linux based solutions, Ascend, Lucent, Cisco, devices such as the SonicWall family of firewalls, McAfee VirsuScan, Norton Antivirus, Norton Personal Firewall, ZoneAlarm, and dozens of others. Ten years ago, firewalls were complicated, expensive, and primarily utilized at network perimeters. As technology has improved, prices have fallen and have become easier to implement. Security concerns, however, have also increased dramatically especially with the introduction of broadband Internet access such as DSL and various cable modems. The frequency of new computer security holes and the rate at which they spread have also increased dramatically. With the increase of security concerns, more and more computer network and computer security experts are recommending layered security, even for home users, such as a hardware-based router/firewall device coupled with a software-based personal firewall, AND of course good

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

updated antivirus software. Good data backup procedures and good password policies, although not specifically addressed in this paper, are also critical for computer security.

Knowing all there is about computer security is very difficult. In addition to knowing and understanding operating systems and applications one must also understand most of the following: Java, Javascript, ActiveX, FTP, Passive FTP, IP, TCP, UDP, IRC, NNTP, SSL, TFTP, DHCP, DNS, Finger, Ident, Kerberos, LDAP, WINS, whois, POP3, SMTP, ping, traceroute, AURP, BGP, EGP, IGMP, OSPF, RIP, SAP, IPSEC, IKE, PPTP, telnet, and thousands of others (or at least to know how to get useful information on). There are also some of the newer Internet applications such as Napster, Aimster, AudioGalaxy, Gnutella, imesh, Scour, Morpheus, AOL Instant Messenger, MSN Messenger, Yahoo! Messenger, Battle.net, Diablo II, Doom, Quake, Yahoo! Games, and thousands of others that can potentially open your computer and computer network to computer security holes. If you want proof, install some of these applications, open a Command Prompt window, and run "netstat –an". This will list all the open and listening ports; do you recognize all of them? Additionally, a newer application called Wrapster allows anyone to "wrap" any file into a MP3 file for transmission via most of the new peer-to-peer file sharing applications such as Morpheus. Norton Antivirus has alerted me of the SubSeven backdoor embedded in both an MP3 file and an MPEG file! Without changing the default antivirus setting from scanning program files and documents as recommended, to scan ALL files, I am not sure I would have been protected in these cases!

Definitions

Some of the terms mentioned in this paper and other terms you will encounter in your search for more knowledge related to computer security can be researched at www.whatis.com (or http://whatis.techtarget.com), http://www.pcwebopedia.com/, or http://www.dictionary.com/ .

Implementing your Layered Security

Layered Security, Layer 1, Selecting your Antivirus Software

A good antivirus software program, properly configured and properly updated, running on all of your computers whether they are workstations or servers is a must, and a starting point for computer security. If a product has been certified by an organization such as ICSA (http://www.icsalabs.com/), you should be more secure or at least more comfortable with your choice. Remember, the important factor is the multiple layers of defense.

Based on dozens of articles, reviews, comparisons, and personal experience, I have listed the following antivirus programs in order with the highest recommended at the top of the list. As long as you keep your antivirus software updated, there is most likely very little difference between all of the following quality programs. Features and the actual performance of the computer virus handling are much more important than price and as always, research the product to make sure it works correctly with your operating system and backup before installing.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Norton Antivirus (http://www.symantec.com) ICSA Labs Certified - $50
McAfee VirusScan (http://www.nai.com) ICSA Labs Certified - $38
Panda Antivirus Platinum (http://www.pandasoftware.com) ICSA Labs Certified - $59
Trend Micro PC-cillin (http://www.antivirus.com) ICSA Labs Certified - $30
Norman Virus Control (http://www.norman.com) ICSA Labs Certified - $59
F-Secure Antivirus (http://www.f-secure.com) ICSA Labs Certified - $125
Sophos Antivirus (http://www.sophos.com) ICSA Labs Certified - $60
AVG Antivirus (http://www.grisoft.com) ICSA Labs Certified – FREE
Computer Associates Inoculate IT (http://www.ca.com) ICSA Labs Certified – network pricing

Layered Security, Layer 2, Selecting your Personal Firewall Software

The next layer of defense protects you from anything that might get through your other layers of defense. An example might be SubSeven Pro which most antivirus software does not even recognize. Microsoft is even recently recommending personal firewall software. "Install a personal firewall application. A personal firewall is like a valve that lets you access the Internet, but prevents the Internet from accessing you. The firewall simply masks from the Internet all the information and activity that is on your side of the modem. Firewall software can also alert you if and when anyone tries to break through that wall to access your computer."[5]

Based on dozens of articles, reviews, comparisons, and personal experience, I have listed the following personal firewall programs in order with the highest recommended at the top of the list. Personal firewalls do have a greater variation in features and security capabilities than antivirus software. Even more so than with antivirus software, features and the actual performance of the computer virus handling are much more important than price. For the latest comparisons and reviews check out your favorite technology web sites or publications.

ZoneAlarm (http://www.zonelabs.com) - FREE or ZoneAlarm Pro for $40
BlackICE Defender (http://www.networkice.com) - $40
McAfee Firewall (http://www.nai.com) - $30
Sygate Personal Firewall (http://www.sygate.com) - $20-$48
Tiny Personal Firewall (http://www.tinysoftware.com) - $37
Norton Personal Firewall (http://www.symantec.com) - $48
Windows XP Internet Connection Firewall – comes with Windows XP

Layered Security, Layer 3, Selecting your Router/Firewall Device

"Our Blue Ribbon Award goes to the SonicWall SOHO: It contains the right mix of features, price and ease of use for this target audience. While it could still use some improvement, particularly in terms of its documentation, it's the best of the bunch. And at $495, it represents a terrific value."[6] Although I have occasionally locked-up the SonicWall SOHO/10, based on this model only handling 3072 concurrent sessions, I would recommend it or a similar SonicWall

[5] Newburger, http://www.microsoft.com/privacy/safeinternet/topics/connecting.htm
[6] Strom, http://www.nwfusion.com/reviews/2000/0807rev2.html

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

device to anyone who asked! Unless you are running an application similar to Nmap or Nessus, 3072 concurrent sessions should be adequate for a home, home office, small business, or telecommuter firewall. It has been the most secure and most stable layer in my computer security arsenal. If you require more users or more concurrent sessions the SonicWall Pro VX supports and unlimited number of users and up to 30,720 simultaneous connections.

There are several other good devices out there and depending on features, support, warranties, documentation, ease of installation and configuration, security, and costs you might choose another device. These types of devices do not need updates every year in order to still function, unlike antivirus software, so consider that along with the cost. It is still a good idea to check for firmware updates for these devices. All of the devices do not give full firewall features and capabilities so research your product carefully. The true firewall features seem worth the additional costs compared to those that really just perform NAT. The devices most often advertised and the less expensive devices primarily give you NAT/router capabilities only, not true firewall features. If you frequently connect to other networks or systems, VPN capability is strongly recommended and is an upgrade to some of the devices listed below. Furthermore, if a product has been certified by an organization such as ICSA (http://www.icsalabs.com/), you should be more secure or at least more comfortable with your choice. Remember, the important factor is the multiple layers of defense.

Based on dozens of articles, reviews, comparisons, and personal experience, I have listed the following devices in order with the highest recommended at the top of the list.

SonicWall SOHO2 10 user ISA (http://www.sonicwall.com) ICSA Labs Certified - $412
SonicWall SOHO2 50 user ISA (http://www.sonicwall.com) ICSA Labs Certified - $829
WatchGuard Firebox SOHO 10 users (http://www.watchguard.com) - $345
NetGear FR314 Cable/DSL Firewall Router 8 users (http://www.netgear.com) - $210
Ramp Networks Webramp 700s 5 users (http://www.nokia.com) - $295
ZyXEL ZyWALL 10 users (http://www.zyxel.com) - $297
3COM OfficeConnect Firewall 25 users (http://www.3com.com) ICSA Labs Certified - $557
Cisco PIX 501 10 users (http://www.cisco.com) - $459
Gnatbox Lite or Gnatbox 1000 (http://www.gta.com) ICSA Labs Certified

Layered Security, Layer 4, Updating your operating system and applications

With all of the new security holes and vulnerabilities that continue to be found, you must also update your operating system, no matter who the vendor. This also applies to your applications, including your browser. Information related to updating your Microsoft operating syetem can be found at http://www.microsoft.com/privacy/safeinternet/security/best_practices/updates.htm. Information related to updating your Linux operating system can be found at the vendor's web site or at http://www.linux.org.

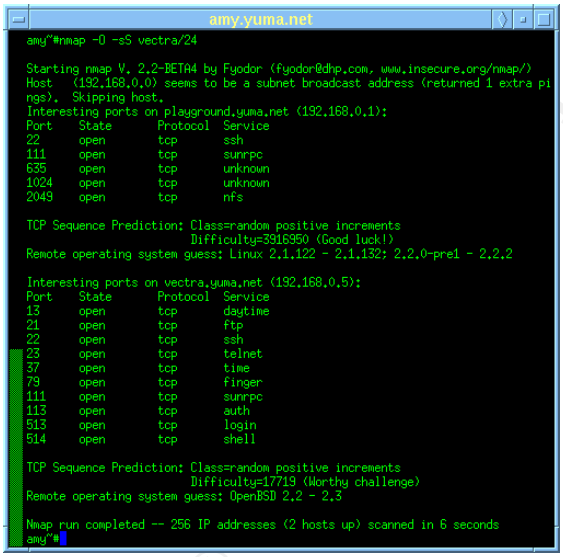
Testing your computer security

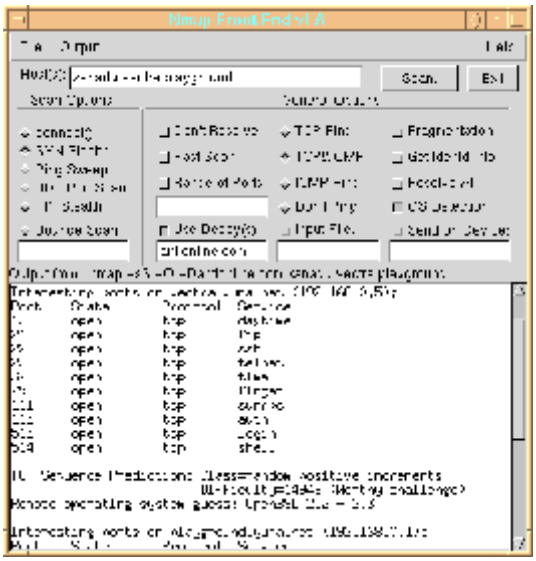
© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

You should periodically test your computer security with multiple resources. Although Linux is NOT the easiest operating system to work with, there are several excellent open source Linux applications that might be worth the time for this type of testing. If you do not have access to a computer loaded with Linux, you also perform simple computer security checks from the following resources: http://www.grc.com where you can read about and choose to run the ShieldsUP! Tests, http://www.dslreports.com where you can also read about security and choose to run the tests in the DSLR Tools menus, http://www.sonicwall.com where you can try the SonicWall Vulnerability Scanning Service, or you also try the Microsoft NT version of Nmap found at http://www.eeye.com/html/Research/Tools/nmapNT.html. These tests should not be able to penetrate your layered security, and should produce timely and easy to understand alerts!

Two Linux applications that are highly recommended are Nessus and Nmap. Nmap can test your your computer or network for vulnerabilities by performing extensive port scans. Nessus can test your computer or network vulnerabilities by performing tests selected for a list of known vulnerabilities. There are commercial alternatives to both of these applications, however, the commercial applications may cost tens or hundreds of thousands of dollars depending on how large your network is and how many users will have access to the software!

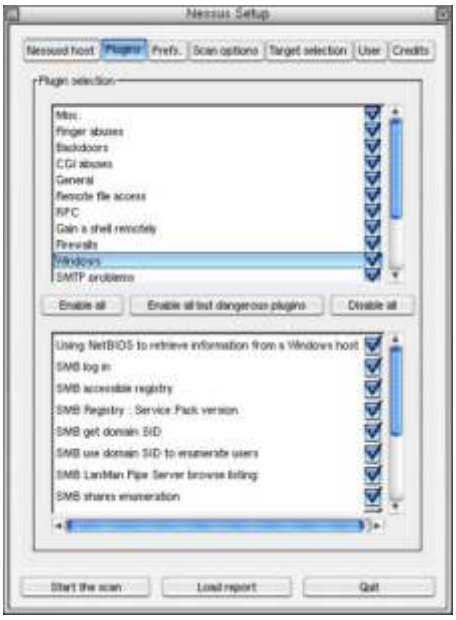
Compared to other port scanners available, and after the Linux learning curve, I feel Nmap is worth a quick review.

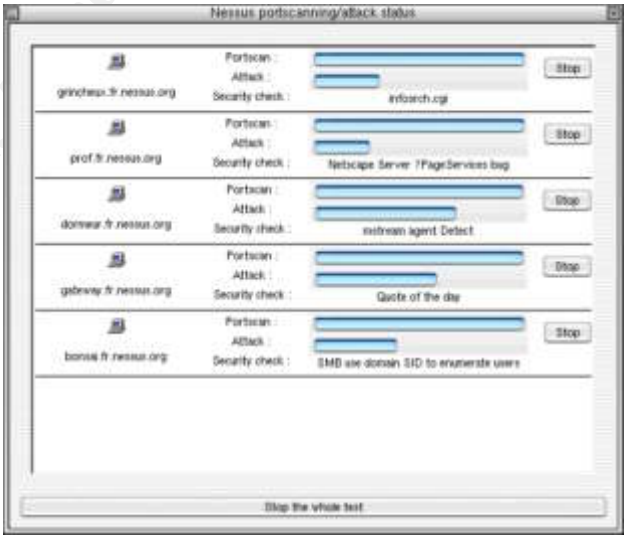




After the learning curve of Linux and Nessus, I have been so impressed with the results that I think it deserves several screen shots shown below so you can see some of the options and the power available in this application.

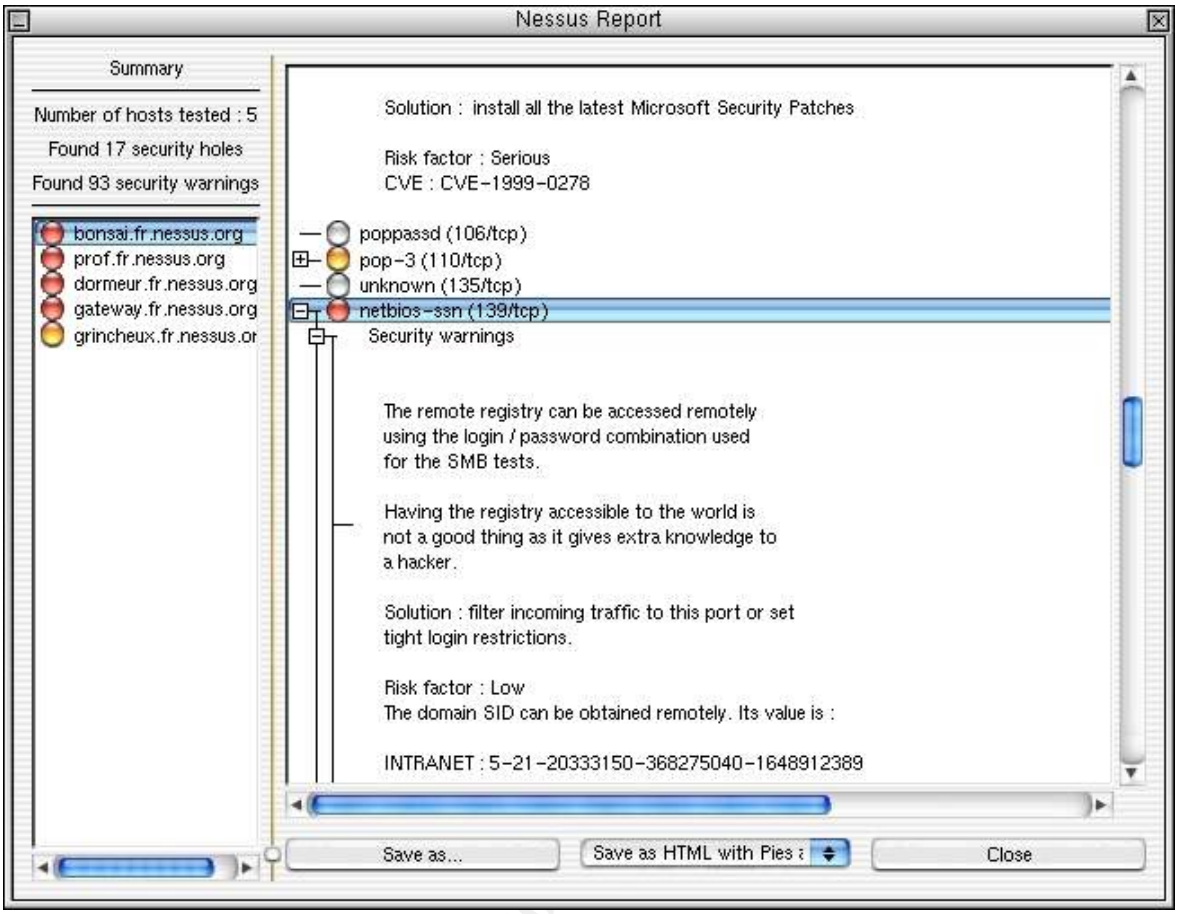
© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.





The four Nessus screenshots above are options and settings that can be customized when you run the vulnerability tests. The larger screenshot below is just one of many pages provided at the end of the testing. It can be saved in several different formats. Depending on options chosen for the tests, the speed of the computer running the test, the speed of the network or Internet connections, and the number of systems scanned, this type of testing can easily take hours or days.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.



Multiple tests from external locations consistently prove that an updated SonicWall SOHO/10, with all inbound traffic blocked (default), was able to pass both an extensive Nmap vulnerability test and a Nessus vulnerability test with ALL plugins enabled. These tests showed NO ports open. Even with all Nessus plugins enabled, there was never a crash or lock-up of workstations protected by the SonicWall. In this case one might assume the SonicWall is sufficient for total computer security protection. It is not and still requires antivirus software and a personal firewall (layered security), plus all operating system and application security patches applied, to be secure.

During my most recent tests utilizing a Red Hat Linux 7.1 machine with Nessus on the same network as a Windows 2000 machine with the Norton Antivirus and Norton Personal firewall, it handled over 262,000 probes at the same time I was editing a Word document and browsing the Internet with very little degradation in performance. The Windows 2000 machine with the Norton Antivirus and Norton Personal Firewall showed the following open when tested locally with Nessus: 135, 137, 139 with a NULL session security hole found, 445, 1025, 1026, 1027, 1028, 1029, was able to identify the operating system, and was able to perform a traceroute to the machine. After disabling “allow local private network”, the same Windows 2000 machine with Norton Antivirus and Norton Personal Firewall still found the following ports open: 445, 1026, 1028, and while improved over the previous test was still able to identify the operating system.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The Windows 2000 machine with the Norton Antivirus and BlackICE Defender running in the Paranoid Protection level showed the following open when tested locally with Nessus: 445, 1025, 1026, 1028, incorrectly identified the operating system, and answered to an ICMP timestamp request. These results may be attributed to configuration rather than the actual security capabilities of the products, however do coincide with other public reviews and comparisons. Although not tested or reviewed to my satisfaction yet, a different machine with Windows XP, RC1, fully patched and running the Windows XP Internet Connection Firewall, performed very well when tested with Nessus showing no ports open!

Summary

"Think of your defences as an obstacle course for would-be hackers. The more hurdles and hazards you can place between them and the things you are trying to protect, the more likely they will be to fail. Your approach, then, should be to design a layered system of defences where various barriers in the form of tools, policies, procedures, etc., work together to make the hacker's job as hard as you reasonably can."[7] To assist with your layered computer security, update your computer security skills and knowledge, constantly with links such as several listed below.

The layers of computer security listed above should give you a secure computing environment. If you want your computer for home, home office, small business, or telecommuting to be secure you must utilize layered security! Although the quality of the product at each layer does matter, **it is more important to have the layers than it is to have the best at each layer!**

Computers utilized in these tests:

Test machine #1
Compaq Deskpro PIII-550
384MB RAM
9GB SCSI
Compaq 10/100 NIC
Windows 2000, Service Pack 2
IE v6.0 fully patched
Norton Antivirus 2001 (v2.56+) fully updated
Norton Personal Firewall 2001 (v7.07+) fully updated
BlackICE Defender also tested on this machine

Test machine #2
DELL Dimension PIII-600
256MB RAM
10 GB IDE
3COM 10/100 NIC
Red Hat Linux 7.1

[7] Crume, p. 15.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Nmap v2.53
Nessus v1.0.9 with latest plugins

Test machine #3
DELL Dimension PIII-600
640MB RAM
10 GB IDE
3COM 10/100 NIC
Windows XP Professional, RC1, build 2505 fully patched
IE v6.0 fully patched
Windows XP Internet Connection Firewall
No antivirus software was tested due to error messages and warnings during installations

Several machines outside of this LAN were also utilized to test the effectiveness of the SonicWall SOHO/10

SonicWall SOHO/10 fully updated connected to Cox@Home Toshiba cable modem
SonicWall is set to defaults, deny all from WAN (outside), allow all from LAN (inside)
10MB hub also utilized for more LAN connections

References

Newburger, Eric C. "Home Computers and Internet Use in the United States: August 2000". P23-207. September 2001. http://www.census.gov/prod/2001pubs/p23-207.pdf (October 7, 2001).

Janss, Steve. "Frontier Defense Keep the Bad guys away from your remote outposts". August 7, 2000. http://www.nwfusion.com/reviews/2000/0807rev.html (October 14, 2001).

Janss, Steve. "Triple your remote office protection". August 6, 2001. http://www.nwfusion.com/net.worker/news/2001/0806networkerreview.html (October 14, 2001).

"Microsoft Privacy and Security Fundamentals". http://www.microsoft.com/privacy/safeinternet/topics/connecting.htm (October 20, 2001).

Strom, David. "Stop 'em with a box Let your remote workers set it and forget it". August 7, 2000. http://www.nwfusion.com/reviews/2000/0807rev2.html (October 14, 2001).

Crume, Jeff. Inside Internet Security, What Hackers Don't Want You To Know. Addison-Wesley, 2000.

http://www.sans.org/top20.htm - The Twenty Most Critical Internet Security Vulnerabilities (Updated) The Experts' Consensus

http://www.cert.org/tech_tips/home_networks.html - CERT Home Network Security

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

http://www.nipc.gov/warnings/computertips.htm - Seven Simple Computer Security Tips for Small Business and Home Computer Users

http://www.solarwinds.net/ - SolarWinds Network Management and Discovery Software

http://www.foundstone.com/index.html - SuperScan port scanning software

http://www.insecure.org/nmap/ - Nmap port scanner or network exploration software (FREE, great, can be complicated to install and configure)

http://www.eeye.com/html/Research/Tools/nmapnt.html - Nmap for Windows software

http://www.nessus.org/ - Nessus computer security scanner software (open source, FREE, great, can be complicated to install and configure)

http://www.snort.org/ - Snort Intrusion Detection software (open source, FREE, great, can be complicated to install and configure)

http://www.dslreports.com/ - DSL Reports has good computer security tests

http://www.grc.com – Gibson Research Corporation has good computer security information and good computer security tests including ShieldsUP! And LeakTest

http://www.sonicwall.com – Excellent and cost-effective firewall products

http://www.zonelabs.com – ZoneAlarm firewall FREE for personal and non-profit use

http://www.networkice.com – BlackICE Defender personal firewall software

http://www.symantec.com – Symantec also known as Norton

http://www.nai.com – Network Associates also known as McAfee

http://www.dynamsol.com/puppet/nukenabber.html - NukeNabber a simple port monitoring software package

http://www.grisoft.com – FREE anti-virus software

http://www.musiccity.com/ - Morpheus, one of the newer peer-to-peer file sharing applications

http://www.icsalabs.com/index.shtml - ICSA certifications for computer security solutions

http://www.foundstone.com/index.html - Foundstone Professional Services and computer security testing tools

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

http://www.securityfocus.com/ - Computer security news and information

http://www.scmagazine.com – Excellent computer security publication

Thomas, Kim. "Building a Secure Home Network". July 26, 2001. http://www.sans.org/infosecFAQ/homeoffice/home_net2.htm (October 13, 2001).

Krein, Derek. "Layers of Defense for the Small Office and Home Network". July 24, 2001. http://www.sans.org/infosecFAQ/homeoffice/layers.htm (October 13, 2001).

Burden, Mike. "Security Essentials for the Home Network". May 2, 2001. http://www.sans.org/infosecFAQ/homeoffice/home_net.htm (October 13, 2001).

McDougall, Bonnie. "Personal Firewalls – Protecting the Home Internet User". August 17, 2001. http://www.sans.org/infosecFAQ/firewall/home_user.htm (October 13, 2001).

Hillman, Dale. "How Complicated Is Home Protection?". November 23, 2000. http://www.sans.org/infosecFAQ/homeoffice/protection.htm (October 13, 2001).

Baker, Andrew S. "Connecting Your Home LAN to the Internet – Securely". March 27, 2001. http://www.sans.org/infosecFAQ/homeoffice/home_LAN.htm (October 13, 2001).

Johnston, Mark. "DSL (Defending Someone's Lair) in the 'Always-On' World of High-Speed Internet from the Home". October 11, 2000. http://www.sans.org/infosecFAQ/homeoffice/DSL_home.html (October 13, 2001).

Heyn, Frederick M. "Batten Down the Net Hatches: Making Your 24x7 Home Access to the Internet as Secure as Possible". May 9, 2001. http://www.sans.org/infosecFAQ/homeoffice/hatches.htm (October 13, 2001).

Deterding, Brent. "Nmap - The Tool, It's Author and It's Implications". July 13, 2000. http://www.sans.org/infosecFAQ/audit/nmap.htm (October 13, 2001).

Zych, Tina. "Personal Firewalls: What are they, how do they work?". August 22, 2000. http://www.sans.org/infosecFAQ/homeoffice/personal_fw.htm (October 13, 2001).

Pasetta, Mike. "High Speed Security at Home". April 10, 2001. http://www.sans.org/infosecFAQ/homeoffice/high_speed.htm (October 13, 2001).

Zimmer, Kevin. "Protecting Your Company from the Small Office or Networked Home Office". February 12, 2001. http://www.sans.org/infosecFAQ/homeoffice/protecting.htm (October 132, 2001).

Maxon, Keith D. "Application Layer Firewalls vs. Network Layer Firewalls: Which Is the Better Choice?". August 13, 2000. http://www.sans.org/infosecFAQ/firewall/firewall.htm (October 13, 2001).

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Tang, Ted. “Basic Home Computer Internet Protection for Free!”. November 18, 2000. http://www.sans.org/infosecFAQ/start/free.htm (October 13, 2001).

Davis, William. “Firewalls: What I Wish I'd Known When I Was Getting Started”. September 20, 2000. http://www.sans.org/infosecFAQ/start/fw_start.htm (October 13, 2001).

Kisser, Scott. “A Hardware Based Firewall Option for the SOHO (Small Office/Home Office) User. A look into the LINKSYS Etherfast Cable/DSL Router.” December 4, 2000. http://www.sans.org/infosecFAQ/homeoffice/option.htm (October 13, 2001).

Ashworth, Robert. “Protecting your Home Computer from the Internet, Can You Keep the Heat Out?”. December 9, 2000. http://www.sans.org/infosecFAQ/homeoffice/heat.htm (October 13, 2001).

Giannoulis, Peter. “Are Firewalls Enough?”. September 11, 2000. http://www.sans.org/infosecFAQ/firewall/firewalls_enough.htm (October 13, 2001).

Epifanoy, Pavel. “Personal Firewall: Pros and Contras”. November 16, 2000. http://www.sans.org/infosecFAQ/homeoffice/personal_fw2.htm (October 13, 2001).

Simmons, Craig. “Firewall Network Appliance”. October 10, 2000. http://www.sans.org/infosecFAQ/firewall/fw_netapp.htm (October 13, 2001).

Alimagno, Archie. “My Personal Firewall Failed, What Do I Do Now”. November 14, 2000. http://www.sans.org/infosecFAQ/win/failed.htm (October 13, 2001).

Lutheran, John. “My Home Setup”. July 2, 2001. http://www.sans.org/infosecFAQ/homeoffice/setup.htm (October 13, 2001).

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 22nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**