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.

Building a Secure Home Network

Maintaining confidentiality and integrity of your data should always be of critical importance. Anytime your computer is connected to any other computer, or opens software provided on media (CD, disk, etc..), you are exposing yourself to possible viruses, malicious code, or hackers looking for information. An unsecured computer connected to the Internet is much like leaving your front door wide open when you go on vacation. This paper discusses the implementation of a multi-layered secure home network including, virus ...

Copyright SANS Institute
Author Retains Full Rights

AD
Symantec™
Endpoint Protection 12
The next generation of reputation-based security
Download the beta
Symantec.
Confidence in a connected world.

Building a Secure Home Network

Kim Thomas
GSEC V1.2c

Is your computer/network secure? Whether a person has one computer or a dozen connected to the Internet, the dangers are the same. An unsecured computer connected to the Internet is much like leaving your front door wide open when you go on vacation. The temptation is too much for curiosity seekers, and hackers looking for open doors. Even placing locks on your door is not enough, given the increased dangers of viruses and worms.

As long as there have been home computers and as long as people have been able to share files and data via BBS's, floppys, tapes, there have been viruses. Long before Internet email was commonplace, viruses still invaded corporate America. The source was renegade programs and document macros carried by diskette. The volume and types of files that are shared have increased. Where once, mostly text files and documents changed hands, now there are hundreds of file types including pictures, MP3's, etc

Even today, when the threat is greater than it has ever been, many people leave their network open to hackers and sniffers looking for information.

What? Educate me… What does it mean to be secure?
Anytime your computer is connected to any other computer, or opens software provided on media (CD, disk, etc..), you are exposing yourself to possible viruses, malicious code, or hackers looking for information.

There are many different methods of locking out intruders from invading your systems. Simply using one method may not be enough to protect you from persistent intruders. Also, there are levels of protection. How much protection do you need? That depends on how many systems you are trying to protect, what kind and valuation of the data on the systems.

Just like in the real world, security is only good if the tools are used. Condoms provide many different types of protections during sex, but many refuse to use them. Locks on cars and homes are provided to keep intruders out. Then why do some people leave their homes and vehicles unlocked? Is it because they don't understand the threats? Is it because they believe they have nothing of value to be stolen? Or are they simply ignorant to the risks?

Your computer has tons of data collected about you. It keeps track of where you have been, what you have been browsing, who you are, personal information, bank account numbers, passwords, email, identity, etc…. Leaving your computer open and unsecured allows intruders to view every detail about you, not including the threat to personal properties. Some attacks can cause damage to your system and your data making that information inaccessible to even you, the owner.

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

Even a secure home is never completely safe. Intruders break in or find back doors or loose windows. The same is true of your computer network. Hackers search for open doors to nudge their way through, others deploy agents or scanners set to check every loose connection to find a way in.

What do these people want with me? Why would they bother?
In some cases, hackers set out highlight vulnerabilities in software programs. The results of these attacks are not always malicious in nature, but more like the common vandal. A vulnerability is a back door or a bug in a software program that defeats the functionality of the program. It could allow intruders to get through undetected, cause erroneous results or Denial of Service (DoS) attacks or any other of a number of different problems.

A hacker wishing to disguise himself can even use your computer and identity to unleash a malicious virus, costing billions of dollars in cleanup and have the virus traced back to you.

Attacks are not always personal in nature. There are almost as many reasons for attacks as there are attackers. It's better to protect yourself so that you are not a victim.

OK I am convinced! How do I secure my network and make it safe?
1. Adding Network Adapters and limiting the protocols
Whether you are adding dial-up adapters for your modem or Network adapters for your internal or external NIC cards, you want to be certain to bind TCP/IP only to the external adapters. Most importantly, all network services (like Microsoft Logon, File and Print Sharing, and Client for Microsoft Networks) should NEVER be bound to TCP/IP to prevent unauthorized access. So where do I bind them? The Network services should only be bound to the Netbeui protocol, and optimally the local network adapter, if possible. Shield's UP provides an excellent tutorial that highlights these essentials.

It is always dangerous to bind NetBIOS over TCP/IP since it leaves several dangerous ports used in DoS (Denial of Service) attacks open for abuse. Although more ports represent a problem than these, ports 137 and 139 are the largest problem in NetBIOS attacks.

Port 137 is used for WINS server flooding. Flooding involves the construction of many packets of random size and contents sent to UDP port 137, thus overloading the port. The constant bombardment of bad packet information causes the WINS server to fail after about 5 seconds, thus resulting in a denial of service to all machines connected to that server.

Port 139 is another NetBIOS port used in DoS attacks. Attackers construct partial packets with the urgent flag set, and repeatedly send them to the target machine. Windows does not know how to handle this type of malformed request. Depending on

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

the operating system, this attack may have varying effects on the machine, most resulting in the machine requiring a reboot.

Network I.C.E. provides a Port Knowlegebase that lists ports with their most common assignments and links to more information. There are also links to other resources for detailed listings of ports used by Trojans.

2. Protect yourself from renegade viruses

Computer viruses are just like those in the real world. You would not risk your life not being vaccinated against viruses with a known prevention just like you should not leave your computer system open to potentially harmful viruses as well. The risk of computer infection has been rising steadily. According to PC World, "Five years ago, the chance you'd receive a virus over a 12-month period was about 1 in 1000; today, your chances have dropped to about 1 in 10" [1]. The leading anti-viral tools are Norton's Anti-Virus and McAfee VirusScan. Experts recommend updating virus definitions once a week and scanning your PC for viruses. Most virus protection programs allow for an automated means of scanning your PC. You can schedule this scan for hours when no one will be at your PC so the scan does not interrupt prime working hours and you can be at ease in knowing that your system is free from viruses. If a virus is found, most anti-viral software has ways of fixing, trapping or eliminating the virus from your computer. Keep in mind that viruses can have adverse effects on your files and can corrupt data beyond repair.

3. Use a Personal Firewall

What is a firewall? A firewall is a way of controlling traffic coming into and leaving your PC. Based on rules that you can configure, you can determine what is acceptable, low-risk traffic vs. high risk security breeches. Firewalls allow you to monitor the requests coming into your PC and provide alerts at unauthorized accesses. Some internet sharing software provides limited firewall capabilities built into the product. Sygate, for example, offers a built-in network firewall with Sygate Home Network . For more complete protection, they also provide Sygate Personal Firewall, free of charge for personal use. Another good free software based firewall is ZoneAlarm. Both Sygate and ZoneAlarm allow you to set policies, capture traces of who is snooping in on you and allow you to configure what traffic is allowed in or out of the machine.

4. Invest in a good router w/firewall built in

Another alternative to the software based firewall is to purchase a router. Today, routers are available in almost every configuration (Cable, DSL, dial-up). The router acts like a shield to your network. The router sits between your home network and your connection to the internet. Thus, the connection to the internet is made by the router. The router is set up with the IP information required to make your connection to the internet. The router knows about your home network and acts just like another computer with its own IP Address on your Local Area Network (LAN) and can communicate with each of those machines. All internet requests made by any machine

[1] Zetter, Kim, "How a Computer Virus Works", 23 October 2000, URL: http://www.cnn.com/2000/TECH/computing/10/23/virus.works.idg/

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

on your network are forwarded to the router and then out into the internet. Likewise, any traffic trying to sneak into your network gets intercepted by the router first and is forwarded to its destination. The advantage to a router over other forms of security is that no computer on your network is directly connected to the internet.

5. Use good strong passwords

Passwords are very important in the protection of your systems and your data. Your goal in the protection scheme is to make it as difficult as possible for people to guess their way into your files. Your name is not an adequate password, not is the name of your dog or your cat or your spouse. Dictionary words as passwords make very easy passwords to crack. When constructing a password, use as many different types of case, characters, numbers, symbols and interleave them. TOY@@@@@ or Toy12345 do not make a strong password, but 3T@@oY#8 makes a much stronger password. Also, its important not to make common substitutions for letters. If "Silo" does not make a good password, "Sylo" won't make any better or stronger one. Password breakers try these common substitutions to find weak, poorly constructed passwords. Protect everything important to you. The table below illustrates the speed by which passwords can be decrypted, given their construction.

Password Type	1 char.	2 char.	3 char.	4 char.	5 char.	6 char.	7 char.
All lowercase	4 ms	11ms	166ms	4s 495ms	1m 24s	47m 21s	23d 34 h
Upper and lowercase	5 ms	29ms	1s 378ms	1m 9s	57m 47s	2d, 3h 44m	109d 18h
Upper, lower, and numbers	5 ms	40ms	2s 288ms	2m 20s	2h 21m	6d 2h 55m	More than a year
Upper, lower, numbers, and symbols	5 ms	86ms	7s 925ms	11m 45s	18h 48m	82d, 16h	More than a year

[2]

6. Use Special Care with Sensitive Data

Do you run a webserver from home? Share up all those MP3's with Napster or another mega-share tool? By doing so, you make that PC more vulnerable and more open to attack. Don't be careless. If possible, secure information accessible through those tools to another hard drive or at least another logical drive. Don't store other system critical or personal files alongside shared material. Use passwords on all file shares. Don't share whole drives, but limit sharing to the files or directories needed. The point is to not make yourself more of a target than you already are.

7. Backup Frequently

Even though we have explored all the ways to secure your system, incidents happen. Make sure you back up all critical, system and data files often. Make a data image of the drives. If you are hacked and files are destroyed or corrupted, having good backups can bring you back online quickly and without too much difficulty and without loss of critical data. Backups are like an insurance policy. You pray that you never need them. Having them, though, may be priceless if you are storing the data you may never be able to fully recover.

---

[2] Manville Schools, "Creating Strong Passwords" URL: http://www.manvilleschools.org/hrd/Creating%20strong%20passwords.htm

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

8. Use encryption where necessary

There are ways that email can be intercepted in route or disguised to appear as though they came from another sender. If you are sending sensitive information that could be damaging to either party if intercepted, you always want to make a point to use Private-Keys and encrypt the email. That way, you, the sender and the recipient can be guaranteed that the email has been delivered intact, know who the email came from, and that only the sender was responsible for initiating it.

9. Utilize safe-surfing and know what you are installing

How many times have you come upon a web site and had an installation box pop up? This site is better viewed when *xxx* installed? ACK!! Never blindly install from one of these sources UNLESS you really know what you are installing and from what source. Unsuspecting and non-security focused individuals who install these applications may be installing a trojan or other "spyware" on their computers. Spyware basically creates a pathway for an attacker. It allows them to monitor everything that goes on inside your computer.

So, how do you keep your browser safe? Go to Tools=>Internet Options and click on the security tab. Click on the Internet zone and press Custom level. This allows you to control by risk or individually options which could affect your computer. There are three default levels of security, Low, Medium and High. Setting your security level to Low is not advisable. Low turns on most options, and could leave your computer standing out there on the internet nearly naked. This could leave your computer ripe for security invasions. Medium security turns off some of the security risk options and leaves some options on. Medium security is recommended for trusted sites. A trusted site is a site which you define as being trustworthy not to contain any harmful material. High security is the recommended option for all sites which you have not deemed as being trustworthy. High security disables most options and locks down the browser. Internet Explorer also allows you to configure each zone by whatever custom criteria you set. It allows you to Disable, Enable or Prompt for many of the settings.

Some of the options which are custom set are described below with the recommended settings for optimal security. Unless you have a specific reason to enable ActiveX for a specific site, ActiveX should almost always be disabled. ActiveX controls can be written to write and interact with the users hard disk and can cause severe security problems. Disable all scripting. This will prohibit potentially dangerous VBS scripts from executing and installing renegade viruses or worms and/or causing damage to your computer. Disabling all cookies can prohibit you from viewing some web sites. Enabling cookies is a fairly personal option. Cookies allow traces of where you have been and allow web sites to track your visits to a site as well as allowing them to provide personalized content. If you are really concerned about what cookies you accept, you can set these options to prompt and everytime your browser encounters a cookie, you will be asked whether or not you want to accept it. Most other options should be set to disabled or prompt.

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

Remember, your system is only as safe as the options you select. For optimal security, set all sites to High and then you can reset options if you encounter problems while browsing.

Also, given that Outlook and Outlook express also allow HTML content in their email applications, be certain to set some of the same precautions in your email clients. VBS scripting should always be disabled.

I have secured my system! Does this mean I am safe? Do I need to worry anymore? Am I safe?

No one is ever completely safe. New vulnerabilities are found every day in all operating systems, new ways are found to sneak past security gates, and new ways are found to break secure key algorithms. A locked door is a challenge and an invitation to hackers. All of these tips above will help, but nothing should ever be considered as a guarantee that no intrusions will ever take place.

Now that you have followed all these steps, there are sites out there to test your visibility and vulnerability. If these tests still identify open holes, it's a good idea to follow their recommendations. Gibson Research Corporation's Shield's Up performs a thorough test and provides a good analysis. Symantec provides a free Symantec Security Check too that tests for a number of categories of vulnerabilities and provides statistics so you can see how your system fared compared to the others who have taken the test.

Maintaining confidentiality and integrity of your data should always be of critical importance. Do not share passwords with others and certainly don't open up full drives unless there is a specific need to do so. Always password protect sensitive material.

For the most in detailed information on setting up security, bugs and vulnerabilities, precautions, etc…. visit Carnegie Mellon's CERT coordination center. The CERT provides information on how to prevent problems, what security problems could potentially affect you and training and education.

The most important point to remember is to never get complacent about your home security. Make sure anti-virus definitions are up to date and that you check periodically for security holes and vulnerabilities that could affect you. Security isn't just for corporations, it should be a part of all of us.

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

List of References

Zetter, Kim, “How a computer virus works”, PC World, 23 October 2000, URL: http://www.cnn.com/2000/TECH/computing/10/23/virus.works.idg/

Detert, Ryan, “A Basic Guide to Home Security”, WebReview, 14 January 2001, URL: http://www.webreview.com/2000/01_14/developers/01_14_00_1.shtml

Buschner, Stephen, “Home Network Security: The Basics”, New Voice News, URL: http://www.newvoicenews.com/sep00/buschner.htm

Hallburg, Carl, Pavlu, Michael, “Securing Your Home Network”, SecurityPortal, 18 July 2000, URL: http://www.securityportal.com/topnews/secure20000718.html

“How to use Norton Internet Security on a Home Network”, Symantec, URL: http://service1.symantec.com/SUPPORT/nip.nsf/docid/1999122108584336

Plotnick, Neil, “Network Security Begins at Home”, ZD Net, URL: http://www.zdnet.com/enterprise/stories/main/0,10228,2632962,00.html

Gibson, Steve, “Network Discipline for Windows 9x”, Gibson Reseach Corporation, URL: http://grc.com/su-rebinding9x.htm

“Trojan and Remote Access Service Ports”, DosHelp http://www.doshelp.com/trojanports.htm

“H-57: Windows NT/95 Out of Band Data Exploit”, CIAC, 14 May 1997, URL: http://www.ciac.org/ciac/bulletins/h-57.shtml

Weise, Elizabeth, “Virus Researchers: Internet needs Immune System”, USAToday 19 June 2001, URL: http://www.usatoday.com/life/cyber/tech/2001-02-27-virus-weise.htm

“Computer Virus Infections up 48 Percent”, Panda Software, 21 January 1999, URL: http://www.pandasoftware.com/press/Yahoo02.htm

Bridwell, Lawrence, Tippett, Peter, “ISCA Labs 6th Annual Computer Virus Prevalence Survey 2000”, URL: http://www.trusecure.com/html/tspub/pdf/vps20001.pdf

Symantec Security Check, URL: http://security1.norton.com/us/sc_stats.asp?venid=sym&langid=us&plfid=21&pkj=AMEODATJTUIFJUILCFG

Manville Schools, “Creating Strong Passwords” URL: http://www.manvilleschools.org/hrd/Creating%20strong%20passwords.htm

Sharick, Paula, “TCP vs. UDP Ports”, Security Administrator, May 2001, URL: http://secadmin.win2000mag-asap.com/info/com.duke_secadmin_20561_20561.html?se=ink

Network I.C.E., “Port Knowlegebase”, URL: http://www.netice.com/advice/Exploits/Ports/

Computer Stuff.net, “Configuring Internet Explorer”, URL: http://www.computerstuff.net/security/ieconfig.htm

CERT® Coordination Center, “Windows 95/98 Computer Security Information”, URL: http://www.cert.org/tech_tips/win-95-info.html

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

Last Updated: May 24th, 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