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.

Personal Firewalls - Protecting the Home Internet User

Firewalls were one of the first protectors of computer crime. They were the first step in keeping hackers out of your network. These corporate level firewalls did their job well but they were very expensive. Because of their price, the average home Internet user could not afford to purchase a firewall for their home. Over the past year, several vendors have developed software-based firewalls for the home user. Some of them are even free! These new Personal Firewalls have given the general public a way to give oneself a...

Copyright SANS Institute
Author Retains Full Rights

AD

Personal Firewalls – Protecting the Home Internet User

Bonnie McDougall
GIAC Security Essentials
August 17, 2001

Computer Crime. Everyone has heard the term and most know its meaning. Gone are the days that only the US Government and major corporations are the targets of today's hacking genre. Believe it or not, the average home Internet user is a prime target for all types of computer crime. While computer crime will never stop, one can take preventative measures to hamper most attempts.

Most have heard the terms "Trojans", "Worms", and "Viruses". Until recently (last 2-3 years) this was the most common threat to the home user. There are plenty of products like virus scanners that protect users from these menacing lines of harmful computer code. This is only one line of defense. All users need to be educated on these harmful attacks and intrusions to their systems. This is the best defense of all – EDUCATION. With the millions of users online daily, and the ever popular "always on" high-speed cable and Digital Subscriber Line (DSL) connections, more and more people are harmed by intrusions. Hackers are looking to "crack" your private information. First, they want your tax returns, credit card numbers, personal passwords, bank account numbers, and anything else privy to their needs. Second, they can break into your computer and use it and its high-speed connection to serve as an instrument to perform a Denial of Service (DOS) attack across the Internet. How bad would you feel if you played a role in bringing down an important website? How much fun will it be calling all your creditors telling them it was not you who made all those expensive purchases? All the hassles can be remedied by protecting your home computer from the hacking environment. This is done not only by anti-virus scanners and privacy protectors, but also by installing Personal Firewalls.

Firewalls were one of the first protectors of computer crime. They were the first step in keeping hackers out of your network. These corporate level firewalls did their job well but they were very expensive. Because of their price, the average home Internet user could not afford to purchase a firewall for their home. Over the past year, several vendors have developed software-based firewalls for the home user. Some of them are even free! These new Personal Firewalls have given the general public a way to give oneself added protection while using the Internet. Before one downloads a Personal Firewall, they should have an understanding of how they work.

Personal Firewalls are software tools, a technology, that helps prevent intruders from accessing data on your personal computer via the Internet or another network, by keeping unauthorized data from entering or exiting your system. When on the Internet, information is being sent and received in small units called packets, using the TCP/IP protocol stack These packets contain the addresses of the sender and the recipient along with a piece of data, a request, a command, or almost anything having to do with your connection to the Internet. Not all of these packets are "nice" packets. These packets can contain malicious information that can be utilized to gain access to your computer.

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

The criteria a firewall uses for passing packets along depends on the kind of Personal Firewall you use. The most common type one can find for home use is an application gateway firewall. This can also be called an application proxy. Anything one sends to and from the Internet first makes a stop at the firewall. The firewall will filter packets by IP addresses, content, as well as specific functions of a certain application. For example, your firewall will allow outgoing port 80 HTTP (web surfing) traffic while disallowing incoming port 80 HTTP traffic. A prime example of this is the recent Code Red Worm that scans systems for open port 80 connections with certain vulnerabilities. The firewall will not allow any incoming port 80 packets to bypass its blocking ability, but will allow outgoing port 80 connections, allowing you to browse the World Wide Web and enjoy some surfing. Some personal firewalls allow you to initiate a block to certain IP addresses, never letting them connect to your computer. This can be useful if the same IP keeps trying to hack into the computer.

The installations of Personal Firewalls can be very simple. Often one will encounter a "wizard" that will walk one through the installation. After the installation and a re-boot of the system, any time you use an application to access the Internet, the firewall will prompt you to see if this connection is allowed to access the Internet. Usually one will know if this connection should be allowed like e-mail, web surfing, chatting, and chatting. If one does not recognize the application that is trying to connect, do not allow it at this time. Do some research and try to find out if this connection is valid. If it a valid connection, you can add it at a later date. As one can see, these personal firewalls are easy to install and maintain. Even for a newbie!

As stated before, these Personal Firewalls have many benefits:

- **They can protect your computer from network attacks when connected to the Internet.**

- **They can stop malicious back door programs like BackOriface or SubSeven from connecting to remote systems.**

- **They might help you control "spyware" programs and help stop SPAM.**

- **They help ensure that your computer is not used to attack others. THIS IS VERY IMPORTANT! You do not want your computer to participate in a DOS attack.**

- **They can help stop hackers gain personal information, such as credit card numbers.**

There are several Personal firewalls available to the home user. They come in all different types and varieties. Zone Alarm from http://www.zonelabs.com is a personal

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

firewall, which is free for personal use, but an upgraded version, with added features can also be purchased. For the beginner, this is probably the easiest to install and maintain. This firewall is the cheapest (free!) and probably the most secure. When I scanned my computer against Zone Alarm, no personal was given out and it showed no ports being open! One can easily adjust the security of the firewall and block all Internet connections with the click of one button. The latest version of this firewall has a MailSafe feature that helps protect your computer from viruses written in Visual Basic scripting, such as the I Love You virus. Norton also has a personal firewall, available from http://www.symantec.com/product/home-is.html. This is a purchasable product and it gets the job done. Also easy to install, this one is more difficult to maintain. This firewall also gives out some information like computer user names when doing a scan. McAfee puts out the third most popular personal firewall at http://www.mcafee.com. This too has a price tag; not offered for free. When I scanned the computer against McAfee's firewall, it gave no personal information and only showed I had one port open.

There are a couple of other Personal Firewalls that are available for home use and are free. These firewalls are for the computer savvy. That is, one needs a good understanding on how to configure a firewall. The first product available is from Tiny Software at http://www.tinysoftware.com/pwall.php. This product is easy to install and is free. This firewall is not very user friendly if you do not know what you are doing. I do not recommend this product for non-tech personnel. A second product can be downloaded from Sygate at http://www.sygate.com/free/spf_download.htm. While free (for demo) and simple to install, it too requires a strong understanding of firewalls to allow for full customization of its firewall filter use. As one can see, there are several Personal Firewalls to choose from. A Personal Firewall comparison can be read at http://www.sysopt.com/reviews/firewall/. Here one can review several firewalls and choose the one that best suits their needs.

Nowadays, installing a Personal Firewall is a **MUST!** Computer crime is on the rise and security experts see no relief in the future. Remember, installation of a Personal Firewall is only one step to protecting yourself from the hacking community. Even if you have installed a Personal Firewall, additional steps must be taken to ensure full force protection. Here are a few hints and suggestions:

- **Have a good anti-virus scanner and update it regularly.**

- **Never run any executable files or scripts sent by e-mail, unless you know what it does. Many executable and scripted viruses can look like they came from family and friends.**

- **Disable file and print sharing on your home computer. Your Internet Service Provider can help you accomplish this task.**

- **Keep up to date with security patches for all the programs you have installed on your system.**

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

- **Use common sense while using the Internet. Not all "pop-up" ads are what they say they are.**

- **No matter what your protection level is, back up all your data on a regular basis.**

Even with all these steps in place, one will never be fully protected. Educate yourself about the computer security industry. Sign up for e-mail security lists and read about what's new with computer security. The Internet is a very powerful entity and at the same time, a very dangerous one. It took me about 5-6 hours to research and write this paper. During that time, my Personal Firewall received about 400 attempted hacks on my computer. **PROTECT YOURSELF!**

Just what does one do if they found out they have been hacked or intruded upon? There are several ways a home user can get information to report a hack or intrusion. The first item that needs to be saved and printed out is the Personal Firewall logs. Each firewall you install will have a log that keeps all information about all packets that enter and leave your computer. This is very important! This will help in investigating the hack or attempted hack into your computer. If you are not computer savvy, find someone at your work location that might be able to help you. Often the Computer Security Officer is a good person to start with. Most are willing to help even with an incident on a home computer. Helping these people will most often help reduce attempted hacks into their corporate network, since data is often taken home and is often brought in from home users. My security officer thinks that his corporate users are actually extensions to his corporate network. Getting his or her advice would be an excellent place to start but they are ONLY responsible for the network(s) they maintain. On the other hand, your home Internet Service Provider (ISP) should provide a way to report intrusions and attempted hacks. Few ISP's are very tolerant about hackers and intruders. Since they have very little control on what the home user does, they do have the power to investigate and report the hacks to a higher level. Remember, these ISPs have thousands of users online a probably receive hundreds of reports a day. Please give them a few days to respond to your e-mail. If it comes to a point where your Internet service has been disrupted because of a hack, please call the local ISP help desk and ask to speak to a security representative. Before you send e-mail or call the help desk, you need to do a little investigating yourself. Here are some items your ISP or even your friend at work might ask for. Included are some tips and hints to get this information:

First, gather all the information you can from your Personal Firewall. Most firewalls will give you, a minimum, the source IP address, source and destination ports, date and time and, if applicable, the application that was used (HTTP, FTP, Telnet, SMTP, etc). Second provide your IP address. This can be done by selecting the Start button, click Run, type WINIPCFG and hit enter. This will give you your IP address. Third use and Internet tool such as Sam Spade, which is a free download from http://classic.samspade.org/. *Make sure you download Sam Spade for Windows.* This tool will allow you to do a *whois* lookup on the source IP address. You can also do a *whois* via the web from the following addresses: From the American Registry for

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

Internet Numbers at www.arin.net. This site will give you a whois lookup for all IP address registered in both North and South America. If the IP is not registered in the Americas, the ARIN website will point you to the other 2 main IP registries. These are the Asia Pacific Network Information Centre, www.apnic.net, and The European Registry of IP numbers at www.ripe.net. All these sites will allow you to do a *whois* lookup. Doing a *whois* lookup will return a lot of technical information. This information will include who is responsible for the IP address in question and often will provide contact information. Some look-ups will provide an e-mail address for reporting abuse. Do not send e-mail to this address. You can provide this e-mail to your local ISP and let them report the abuse. If the hack involved some monetary loss or loss of personal private information, please contact your local authorities. The first call I would make would be to my ISP. Give them all the information they ask for. Second I would call my local Police Department. **Please do use the 911 number, as this is not considered an emergency.** Also, give them any information they need. The police often have a computer crime division that will try to help you all they can. After reporting the intrusion, it is a good idea to make a complete back up of your system. This backup can be provided to your ISP or police department if asked for.

There are a few items that you need to know about hacking and reporting this information. Often hackers will loop through many systems before they reach yours. They will mask their IP address as if it was coming from someone else. This is called "IP spoofing" This is the main reason you want to report abuse to your local ISP and or police department and not report this information to the source yourself. These groups should have the technical expertise to trace a hack to its origins. You do not want to be responsible for reporting false information to an ISP or owners of IP addresses that truly did not hack your home computer. Leave this to the professionals. Second, this another great reason to have a Personal Firewall. Without this firewall, you would not be able to gather all the information needed to report this abuse. Even worse, you probably would not know that anything bad has happened at all. Please, take appropriate protective measures. Place a Personal Firewall on your system, install a good virus scanner, update your programs regularly, back up regularly, and educate yourself on the basics of computer security and computer crime. This is no joke! If you have found that you have been a victim of a hack or computer crime, do the responsible thing: Report the incident to your local ISP and if needed, your local authorities. Be a responsible Internet user. Do not open e-mail attachments if you were not expecting it. Be wary of all that goes on around you when surfing the web. Not everything is what it seems. If it seems to good to be true, then it probably is. If it looks like a scam, it probably is. Take the extra time to figure these things out. The few extra minutes it takes to make sure things are true and valid is a lot easier to overcome rather that the hours or days it takes to recover!

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

Bibliography

Scambray, Joel; McClure, Stuart; Kurtz, George. Hacking Exposed, Second Edition. Osborne/McGraw-Hill. 2001. 477-481.

"Personal Firewalls & Security, Protect Yourself and Your Information While You Are Online" The Digital Home Vol. 8 Issue 6. June 2000
http://www.smartcomputing.com/editorial/list.asp?guid=gypkw480&pcatid=&z=z&otid=0&searchqa=1&wordlist=personal+firewalls&searchtype=0

"Personal Firewalls, Protecting Your Personal Computer on the Global Internet" June 2000.
http://www.oit.duke.edu/oit/policy/firewall/

"Personal Firewalls Keep Intruders at Bay", PC World.com, July 2000
http://www.pcworld.com/reviews/article/0,aid,17637,00.asp

Dalton, Curtis "Getting Personal With Firewalls" Network Magazine, January 5, 2001
http://www.networkmagazine.com/article/NMG20010103S0010

Richmond, Robert "Personal Firewall Comparison" November 4, 2000
http://www.sysopt.com/reviews/firewall/

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

Last Updated: June 18th, 2013

Upcoming SANS Training

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

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**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**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 Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**