High Speed Security at Home

SANS Security Essentials
GSEC Practical Assignment Version 1.2d
e-Coast SANS II March 9, 2001
April 10, 2001

Today many people enjoy the luxury of powerful computers and fast Internet connections in their homes. These luxuries have become increasingly affordable and more individuals are using computers and Internet connections to do more things. People are doing everything from shopping, research, banking and of course using e-mail to stay in contact with friends. In short you could say that we have become very comfortable having these systems in our lives, in our homes and housing a lot of our personal information. It is in our nature, once we become comfortable with something, to tend to loose our fears and when we loose our fears, our guard goes down. By letting our guard down we are leaving ourselves wide open to attack from the outside world.

In general, people take their personal security seriously. They know that in their community it might be okay to leave the car unlocked. In one town I know of people tend to leave their keys in the ignition too. These people know that their community is fairly safe because they know their surroundings. When they go to unfamiliar places or places where things are not safe they wouldn't dream of leaving themselves in a vulnerable position.

Well, I don't care where you park your computer, as long as it is connected to the Internet it is not safe! This is especially true for those who have an "Always on" Internet connection such as cable modems, DSL or ISDN connection since the computer is always connected to the Internet. This situation just isn't safe!

What lurks out there

Just as we enjoy our powerful computers with our high speed Internet access, there are many hackers out there who are enjoying them too. Fast computers and Internet connections allow hackers to use their hacking tools more efficiently against your system. Hackers use tools known as robots (bots for short) and spiders. Bots are programs or scripts that scan and launch attacks automatically without their owner's interaction. Spiders on the other hand do not do attacks directly, but act more like a fly on the wall and let their owners know our vulnerabilities.

Sun-tzu, the author of a two thousand-year-old book entitled, Art of War stated the following:

> *"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.*
> *If you know neither the enemy nor yourself, you will succumb in every battle."*

In short, the hackers know themselves and they are learning about you! The typical user at home knows nothing about the hacker. According to Sun-tzu this is very bad for you!

You might be asking, why would a hacker come after me? Well, there are several possibilities.

1. It is probably easier for them to hack your computer and the computers of twenty of your friends to get your credit card numbers and other financial records than it would be to hack into a bank.
2. They might try to use your system to do their dirty work. By highjacking your computer without your knowledge, they are able to use your computer to help hide themselves while hacking into other systems.
3. They might hack your system simply because they can, for the same reason a vandal might spray paint personal or private property.

It is by the same means that your computer uses the Internet that the hackers do their work. The language or protocol for the Internet is called Transmission Control Protocol/Internet Protocol or TCP/IP. A computer configured to use TCP/IP has many "ports" open. A port is like a "pipe" or connection to the Internet where communications are directed. For example when you are using your web browser the data is typically transmitted via TCP port 80. Your computer typically has many open ports and it is these open ports that the hacker is looking for, just like the car with the keys in the ignition!

How vulnerable am I?

It is a simple test if you are running Windows 98, 2000 or NT to see what ports your computer is using. Just type the netstat –a command from the command prompt. This will provide you with a list of what ports your computer is listening to. You may also want to download Leak Test from http://grc.com/lt/leaktest.htm. This utility will detect and display your vulnerability. Another utility, SuperScan can be found at http://www.foundstone.com/rdlabs/tools.php?category=Scanner. Now that you know the hackers are trying to attack, you need to learn how to protect yourself.

Preventing the Hacker

Or should I say "trying" to prevent the hacker. It seems that as fast as we can put up brick walls, there are hackers out there finding pin holes to start poking at. Even so, it is best to have a wall they have to poke at rather than leaving the door wide open. There are three main types of protection that I want to talk about. The first two are firewall options and the third is virus protection.

With regard to firewalls, there are two main types available. The first is hardware based, meaning there is a special box you put in between your computer or network and your Internet connection. The second is a personal firewall application that you install on your computer.

The Router

When using a hardware solution, commonly referred to as a router, there are several features that are readily available and are desirable.

1. NAT (Network Address Translation): This allows you to hide a private network behind your public internet address
2. DHCP (Distributed Host Control Protocol): This allows a device to receive its network address from a server, it may be desirable to have your router be both a client and a server.
3. DMZ (De-Militarized Zone) sometime referred to as NAT Server: This enables certain Internet traffic to translate your NAT interface and enter your private network from the Internet. Usually this is for allowing specified traffic into your personal network, such as web traffic on a personal web server.

There are many venders that offer these types of routers, such as SMC and Linksys and Netgear. With out getting into vender specifics, here is how you basically want to configure these types of boxes and why.

You will want to enable DHCP for ease of use. This allows your PC(s) to be automatically assigned an IP address when it boots up. If you do not have a static IP address assigned to you from your ISP, you will also want to enable the router to be a DHCP client on the interface that is connected to your cable modem or DSL equipment.

It is also very important to enable NAT. This will do two very key things for you. First, it will allow you to operate more than one computer simultaneously on your Internet connection (a big advantage on it's own). It will also masquerade your computer(s) so that no one from the Internet will be able to see it directly. This is key to your security. If they can't see you, they can't hack you!

Next you will want to make sure to set the router's passwords, do not leave them set to defaults. You will also want to disable telnet from the interface that is connected to the Internet. This will prevent hackers from trying to gain access into your router. You will also want to disable SNMP (Simple Network Management Protocol) from the port that is connected to the Internet. This will disallow hackers from trying to manage your router from the Internet. If your router supports SNMP and you are not able to turn it off, I recommend that you use the NAT server feature and set it to an address that you will not be using on your network. This will essentially black hole any SNMP request, preventing the hacker's attack. This principal can also be used for telnet if you are unable to turn it off. You will also need to configure the default gateway for your router and any DNS entry you might have.

Once this is done you have set up an excellent firewall for yourself. Here is how is basically works. From your private network, your computer will be able to receive an address form the router's DHCP server that it can use to talk to the router and other devices on your private network. If your computer's traffic is destined for the Internet, the router uses NAT to translate your private address to its public address and off you go. The router maintains a table so that it knows where to send packets on their way back from the Internet. Should a hacker try to probe your public IP address looking for your computer vulnerability, there will be nothing to see.

The Personal Firewall

If you are unable to use a router or if your computer is in a DMZ you will want to take advantage of a personal firewall program. There are many to choose from and all of them have their pluses and minus, and all of them provide protection. A few of the leaders to consider are NetworkICE's BlackIce Defender, Symantic Corporations Norton Personal Firewall, McAfee's Privacy Service or Zone Lab's Zone Alarm.

These applications typically enable you to block specific types of traffic from your computer. You can either configure them to block specific internet addresses or traffic or have them automatically block and alert you when they detect suspicious network traffic that is coming to your computer. Some of these applications also provide an intrusion detection system, thus informing you when they see suspicious activities coming from a foreign host. Most of these utilities can be set up very easily and do not require a network security specialist to make them effective.

Anti Virus

Lastly it is recommended that you maintain an anti-virus program. Even though you have a firewall, it is still possible to get a virus or other hacker's tool infected on your machine either though an e-mail, floppy disc or CD-ROM drives. You might also want to test your anti-virus software by using Eicar's anti-virus test utility, which can be found at http://www.eicar.com/anti_virus_test_file.htm. This will enable you to see if your anti-virus software is able to detect a virus. I recommend that you read Eicar's web site on the use of this utility before you consider using it. As part of your anti virus protection, efforts should be taken to insure that the virus definitions are kept up to date to insure that you do not get caught by a virus that already has a fix. Many people tend to install anti-virus software and forget about it. It is critical to keep the definition files up to date, thus keeping your software aware of new threats. This may sound silly to mention, but it is also recommended that you allow your anti-virus software to automatically check your files, especially any files coming in from the internet.

As a side note to making sure that you keep your anti-virus software up to date, it is also recommend that you keep your other critical applications up to date too. If you elect to use a hardware router you should check periodically to make sure that your router's software is current. Often time's problems with firmware are found after it has been released and problems or security holes are fixed. If you are running a personal firewall you will want to make sure that you check for updates as security holes are found and fixed and additional hacker strings are added. You should also make it a point to check that your operating system is kept up to date. If you are running a Microsoft Windows 9x you will find a menu under Start called Windows Update that will take you to the a web site that will automatically check your system and make recommendations for updates. I would also recommend that you do not blindly update everything that is suggested. You should read what they are stating has been fixed and/or what enhancements have been made. If you can't find this menu in your Windows environment, you can go to http://windowsupdate.microsoft.com/ and check for updates. Hackers catch many "professionals" because they have not implemented updates to their systems. It seems foolish to be caught by something that has been fixed.

Conclusion

It has been the purpose of this document to educate you as to the dangers that are out there and how you can help prevent problems or losses with your computer. It does take time to implement some of these suggestions and all of them have costs associated with them, but they seldom exceed $300.00. This is inexpensive insurance to protect your computer and your data! Imagine the personal and monetary costs you'd incur if your system crashed while you were surfing the net and wouldn't reboot properly or the next time you get your VISA statement there is a charge for something you didn't authorize. Remember "*If you know the enemy and know yourself, you need not fear the result of a hundred battles*."

References:

URL: http://www.clas.ufl.edu/users/gthursby/taoism/suntext.htm

URL: http://grc.com/lt/leaktest.htm.

URL: http://www.foundstone.com/rdlabs/tools.php?category=Scanner

URL: http://www.eicar.com/anti_virus_test_file.htm.

NetworkICE Corporation “Network ICE Guide To Home Protection”
URL: http://www.networkice.com/products/networkice_guide.html

URL: http://www.networkice.com/products/blackice_defender.html

URL: http://www.symantec.com/sabu/nis/npf/