Global Information Assurance Certification Paper

Building a Secure Home Network

David B Granger
GSEC
Version 1.4b, Option 1
Class Start Date: 2/1/2004
Bloomington, IL
Instructor: Matt Luallen

Abstract

The Internet is inhospitable to unsuspecting users. As hackers gain experience and better hacking tools, their ability to easily compromise thousands of machines will greatly improve. Home computer users are susceptible to hacker and virus attacks because they lack the resources and knowledge for protecting their home networks. Their networks are at risk more than the corporate network. This paper discusses how a home user can design, implement and maintain a secured home network that meets the personal or business needs of the home user. This paper also helps home users better understand what it takes to create a secured home network.

Introduction

Home users need to be educated in secure computing. Consider the number of users on the internet at any given time. It is projected that in 2005 the population online will be just over 290 million.[1] If just a fraction of a percent were open to attack, look at the number of possible computers open for control by a hacker.

The recommendation and discussion in this paper will be limited to workgroups, also known as peer to peer networking. The focus will be a typical home network. It is not necessarily a best practice guide but a call to uneducated users to approach home networking with more thought and research.

The two greatest tools for building a secure home network do require a desire to learn, understand and persevere. One tool is planning and another is research. Once these two tools are mastered the home user is well equipped to achieve his goals of secure computing.

Planning provides a clear understanding of direction and a measure of success once tasks begin. Planning defines clearly; direction, process, resources and contingencies. This makes the effort more efficient and ends with quality results.

Researching is another tool that must be mastered. It is low cost, easily done and provides much towards the success of secured home computing. How do you think most hackers develop skill? They spend hours researching and then apply what they have learned. There are numerous articles to be found on the web. Perhaps there is someone in the computing field who can answer questions. Also, there are many books with great illustrations.

Threats, Vulnerabilities, and Risks

The Hacker's View

The fields are ripe with harvest! There are millions of available computers just ready for the taking, a virtual supermarket of computing power at a hacker's disposal. The possibility of amassing an army of virtual machines to command is unbelievable, waiting to be directed against some capital enterprise or governmental entity. Then there is the wonderful golden pot of identity theft, with so many possible account numbers and credit card numbers to retrieve.

The unsuspecting home user innocently tasks through the net, maybe looking around for some answer to a pondered question. Perhaps there is a youngster playing a war game or instant messaging a friend. Maybe even a telecommuter surfing the web while connected to the company's network - naïve to the premise of what a secured connection actually is all about. Individuals are unaware of the probing, scanning and sniffing, which happens behind the scenes.

General home users don't know about things such as unneeded services, open ports, protocol vulnerabilities, application holes and operating system vulnerabilities. They all desire immediate connection to the big illusive cloud known as the Internet with as much bandwidth and processor power their monthly budget will allow. Many of them become willing subjects of a hacker's control. Look at the thousands of machines used to attack Microsoft.[ii] The ability to build such an army is as simple as analyzing and scanning for a few minutes to uncover any unsecured home computers, determining the platform, what ports are open and what services are running. Finally, picking any one of dozens of possible attacks and unleashing the power of that machine into the hands of someone who knows how to use it.

The Security Analyst's view

Today's technology is changing so rapidly, it is hard for an analyst to keep up. Imagine how overwhelming it is for a home user. The challenge for secure computing in business is increasing as more people connect to work from home using their broadband connection.

Most people don't realize the Internet is the equivalent of a huge network. This means if security measures are not in place, the home becomes open to anyone desiring access. Individuals want secure networks; unfortunately, a lot of home users just leave that to the operating system

or some “higher authority” known as “them”. Many make statements like, “Oh I’m sure Windows has the security I need”, or “I leave security up to my ISP.” ISP stands for Internet Service Provider not Internet Security Provider![iii] This lack of ownership is one of the biggest problems.

An unsecured home network is dangerous. Today there is a real threat of cyber-terrorist attacks. There are many anti-American organizations on the Internet working to amass sensitive information and/or drone computers to use for attacks. How would a citizen feel if they found out their computer was used to attack the US Government?

Visualize the Road Traveled

The typical home computer user needs to know about the road they are traveling on. An untrained attempt at building, securing and connecting a home network is analogous to driving down a road never traveled, in the dark, without headlights and a map.

Then there is the Internet, a very dangerous place these days. Anything from computer pranks to covert malicious attacks on industries, governments, and societies are perpetrated each day from the Internet. Here are some statistics to consider:

- There are many different types of attacks. Listed below are several:[iv]

  Spoofing (Various types) – using fake IP addresses, sending fake packets, generally masquerading with fake information.

  Probes – scanning networks and hosts for information.

  IP Fragment Overlap Attacks – exploiting a bug in TCP/IP stacks.

  Ping o’Death Attacks – sending large packets to hosts.

  Applet Attacks – using applets to launch attacks.

  FTP Attacks – using the FTP protocol for attacks.

  Web Browser Attacks – using vulnerabilities in web browser to attack.

- The number of attacks is growing each year. A 2002 report shows there was an estimated 180,000 attacks in six months;[v]

- According to one study the number of DOS (denial of service) attacks are happening at about 4000 per week;[vi]

- A recent report suggests that 76 percent of all email delivered is spam;[vii]

- Extremely alarming is the number of young people becoming victims of online abuse and manipulation. A paper written by Albert Benschop for the University of Amsterdam, finds the following statistics:[viii]

> "The report of the Internet Crime Forum (ICF) concludes that "about 20% of the children who use chat rooms on the internet have been approached by pedophiles and other unwished-for persons while they were online". A similar survey in the USA: Online Victimization: A Report on the Nation's Youth [June 2000] shows that approximately one-fifth of the youngsters between 10 and 17 had encountered an undesired invitation or approach via the internet."

Yes, this road is full of bumps, potholes and dangerous intersections. If you are a home user wanting to protect your personal data, children's innocence or legal liability then you need to become proactive in your knowledge of home network design and security.

Recommendation

A home network is a group of computers configured to exchange and share resources such as information, applications and communication channels. Home networking can be an effective way to provide all the users in your household with the resources needed for normal family computing tasks.

A typical network could look like the one in Figure 1.

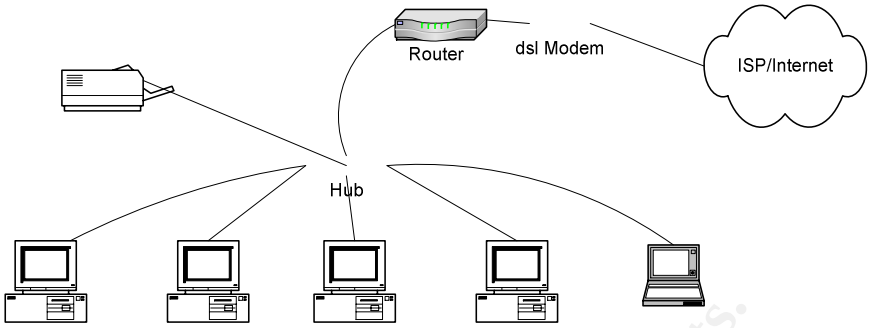

Figure 1: Typical Network

A typical wired network has several desktops or laptops connected to a hub. The hub is used to allow all computers to communicate and use any other resource on the network such as printers. The hub also provides connectivity to the router and modem which are used for connectivity to the Internet.

The recommended approach to building a network is to complete the project by accomplishing several phases. This approach is easier to plan, execute and control.

Phase One

Think about the requirements for this network. Begin to consider such questions as:

Will current equipment be used? If so, how will it be used? Consider the equipment now owned. Maybe with just a few upgrades the existing workstation can be an integral part of the design. Can it become a secondary workstation, one used less than the main home office workstation? One of the children may be able to use it for their needs. It may be decided that the current equipment is not usable and won't be part of the design.

How many workstations will be needed? How will each be used? Today's households have many needs for computing. A mom or dad may need a workstation for home-office use or maybe a docking station for their employer's laptop. Maybe there is a college or high school age child needing access to resources for studies. Perhaps there are gamers in the family who need a workstation. Whatever the situation, determine requirements for the number of units. Yes, all work could be done on one workstation but a network implies multiple workstations.

Where will each workstation be located? This decision will determine not only the availability of each workstation but also the connectivity media used. Most will likely be connected via hubs and CAT cabling. Yet circumstances may warrant a wireless solution. This will dramatically change the design and implications of security for the network.

Who will be the users? What is their capability when it comes to computing? Determine the abilities of the users on the network. This will determine the software and hardware configuration of each workstation. Configuration of firewalls will be established based on the users. Will certain workstation capabilities be locked down? The age of the users will determine if parental control software is needed. The capability of the users will determine how they authenticate and what authorizations will be given to each.

What type broadband will be used? The type of broadband to use is more determined by the area. Digital Subscriber Line (DSL) is a broadband solution which uses existing phone infrastructure for transmission. Typically the provider will charge a fee based on the choice of upload and download bandwidth. The provider will then establish a minimum Quality of Service (QOS) based on the level chosen.

Cable broadband is becoming more common in the home. As providers look to packaged deals, more home users end up going with cable broadband. This broadband is not based on fee for QOS level. Typically a single 6 MHz channel is routed to an individual neighborhood. Based on the amount of other users on the same channel or network, many different levels of throughput will be experienced.

What QOS is desired from the broadband provider? What is affordable? The number of users and budget will be factors in the level of QOS of broadband purchased from the ISP. Keep in mind that the minimum QOS agreement will be approached as more users are on the network.

What provider will be used? What are the choices? Every home usually has a multiple choice of providers. Research each provider; besides the cost of service learn about customer service in times of need. How user-friendly is their setup software and what do they provide for getting started? Talk to other customers of each provider to get an idea of the vendor quality.

What services does each ISP provide? Find out if they provide email service and how it works. Are multiple accounts available for each person in the family or is there one account for the household? Perhaps the vendor provides web hosting services. Maybe the provider offers web

design services needed for a home business. Perhaps the vendor provides storage options.

How can the ISP services be leveraged? Meet with the provider and communicate needs. Perhaps the ISP has spam blocking or maybe they offer firewall software to help you harden your defenses. Whatever the ISP can provide in the way of security only increases the ability to protect assets. Learn what these services are and include them in the requirements.

What sensitive data is there and which workstation will it be located on? The determination of sensitive data is a very important thing to consider. If one of the computers is used for games then the loss of use of this machine would only be a nuisance. On the other hand if one of the computers contains accounting for the past twelve years, past IRS return information, or important account numbers then the loss of the use of this machine would be more critical. The sensitivity of the data on a home computer will be one of the measures of what security controls to use on that machine.

What applications will be used the most? Determining what applications used can help determine which machine to use. This is an availability and/or performance issue. If an accounting application is used by the adults and requires more computing power, then the machine with a good processor and more memory is needed. On the other hand, if there is a graphic artist in the house then the machine with the best graphic processor and monitor would need to be available to this individual.

Will workstations be purchased retail or custom built? Most individuals will purchase retail machines off the shelf. There are many models to choose from and decisions should be based on good research of several models to determine which will best suit needs. With a bit more research one could even determine to build a machine. There are many vendors locally and on the Internet which provide any level “bare system” desired. Bare systems can be found which provide the case, power supply and external drives. Research the motherboard, processor, memory and hard drives to use and then start building. Also, there are bare systems which only require installation of a hard drive and the vendor even provides instructions on how to do that.

How will the network be secured? How to secure the network is the most important question to consider as the list of requirements is drawn out. Time spent in research of this topic will be the most valuable. There are many hours of available reading on this subject. Researching will indicate quickly that security is not just one thing; instead it is a large topic. Included in the references are some sites to help.[ix]

It will be explained later how the security model should consist of several techniques and tasks all working together to stop the malicious acts of others. This is known as Defense in Depth. This technique involves creating several layers of security.

What OS (Operating System) will be used? The majority of households have decided on peer to peer networking with Windows as their OS of choice[x], though Linux is growing in popularity. Whatever the choice of OS; there will need to be time spent in research of the hardware requirements, installation procedures, patches needed, default services that run and the security settings at install.

Other questions could include the following. Will the systems be running 24x7? Does the area have frequent storms? Does the area have a high burglary level? Does the homeowner's policy cover computing equipment? If so, how much is covered? These questions will help determine the physical security needs of the network.

Don't misunderstand; the above discussion of requirements was not an exhaustive list to consider. Each person will have a similar list based on their own situation.

Make a list as questions are answered. This list will give an idea of requirements for design. Include listed statements such as: "I want my network to consist of four workstations loaded with Windows XP" or; "My network will have connectivity using CAT5 cabling." An Excel spreadsheet will work well and could have other columns later used to identify how the requirements are met.

Phase Two

The second phase is researching how each requirement will be met. A good portion of research may be available from the answers to the questions in the first phase. This phase will begin to help focus on design. On the spreadsheet begun in phase one, label a second column; "How", or "How will I accomplish."

Begin to search out the experience and knowledge of others. How did others accomplish what is needed in this situation? Speak to individuals working at shops that build computers and networks or to a specialist working at a local ISP.

Phase Three

The third phase is the design of the secure network. It is best to use graphics. People can grasp design better through graphics. Visio is good to use because of the templates already created. The drag and drop feature works really well. Microsoft WORD has basic blocks and shapes which could work well also.

By this step there should be an idea of a design in mind for the network. Design the network based on resources. After all that is one of the main points of a network, the sharing of resources. Consider each piece of hardware and each application as a resource. Then graphically design how the connectivity and security of those resources will be accomplished. The graphic design will help visualize the intended network. Use this to help focus the building efforts.

The design should be focused on security. As mentioned before the approach should be one of Defense in Depth. A good representation of this approach would be the example of a bank. First, a thief would need to get into the bank through the front door. Second, the thief needs to get past any guards or cameras in the lobby without being detected. Third, they have to get past the teller stations, bank officer desks and usually a locked gated area. Once through all that the vault would be the last obstacle. This layering of security controls is a representation of defense in depth.[xi]

There are many sites available to help understand Defense in Depth. Included in the references are several sites.[xii]

For a network the items to consider for a Defense in Depth approach would be:

1. Keeping up on security updates and software patches

   Because the time between vulnerability discovery and malicious code introduction is steadily decreasing it is very important that a regular update process be established. Microsoft has made this process rather simple. Visit the Windows Update site to initiate an online check of the OS and determine what patches and updates are needed.[xiii]

2. Using antivirus software

   An antivirus software application will help protect computers against many known viruses, worms, Trojans and other malicious codes. It is usually simple to install and maintain.

Purchasing a subscription for definition updates may be required. It is important and recommended to use the default setting of the software for updates. One of the free alternatives is by, Grisoft, Inc. They provide AVG Free Edition for personal use.[xiv]

3. Using a firewall

A firewall can be software on a computer or a hardware device. The purpose is to isolate the outside world from the workgroup. Remember that the Internet is a giant network. Packet traffic can be allowed through or shut off based on several criteria.

For the typical network use a software firewall on the computer with the sensitive data and a hardware device for the perimeter. There are free alternatives in firewalls as well. One example is ZoneAlarm, offered by Zone Labs, Inc.[xv]

Microsoft XP with service pack 2, has a firewall that comes with it. The Windows Firewall, formally known as ICF (Internet Connection Firewall), is enabled by default.[xvi] For XP users this is a good option for a software based firewall.

4. Using strong passwords

Dictionary attacks are common and they are becoming more powerful. It doesn't take long to crack a password based on a common word in the dictionary. Hybrid attacks add numbers and symbols to dictionary words. It is recommended using at least eight characters for passwords. There should be at least one number and one special character. The use of caps and lowercase is recommended also. There should also be a regular period of time when the password is changed.

An alternative to a password is a pass-phrase. This could be a phrase known from a book, poem or song. A pass-phrase is very strong as it has more characters than a normal password and includes spaces. An example would be; "My dog is named Spot." This string has 21 characters making it very hard to crack.

5. Securing file shares

One of the pros of networking can also be a con. File sharing is used to allow network users to read, create, change and delete files based on the access given in the share. Using a firewall will help keep hosts outside the network from sharing files and folders. Windows 2000 automatically grants full control to everyone who can get to shares. Look through the folder/file structure and stop unneeded sharing. Also open shares to created user accounts only as needed.

6. Securing the file system

The steps above will all work towards the securing of files but the use of NTFS allows for even more security. NTFS allows for file level detailed security. Any or all of the users or groups can be kept out of desired files. Authorization can be set on each file allowing a certain user to do some things but not others. It is recommended to use NTFS.[xvii]

7. Securing user accounts

Use strong passwords, disable or delete unused accounts and give only needed privileges to certain accounts. It is unlikely that accounts will be used for malicious attacks if one does the above. If a hacker is able to gain control of one of the accounts and that account has only limited authorization, there is only so much the hacker can do.

Do lockdown the administrator account with a very hard password or pass-phrase. Give administrative rights to those who need it but only use those accounts when needed for administrative work. Instead use an account which has lesser rights for normal use. More information on securing user accounts can be found at two links included in the references [xviii]

8. Securing access from the network

Securing access to a computer which has sensitive data from within the network should be considered. Even if a cracker happens to gain control of one of the less secure machines, they will have a hard time gaining access if there is a limitation on which accounts can get to the data. This can be accomplished using the NTFS file system, user

account management and a software firewall. It is recommended to use all three for this purpose.

9. Renaming accounts

Renaming commonly used accounts makes it less likely for certain attacks to succeed. There are proven, widely used attacks which search for accounts such as Administrator, Guest, Everyone, etc. Renaming these accounts adds to the ability to control what happens on the network. It is recommended to rename the Administrator account to something that would be easy to remember and disabling unneeded accounts like Guest.

10. Disabling unneeded services

There are several services automatically installed and running on computers. These may or may not be needed. Hackers can use certain services to launch attacks. It is recommended to disable or remove unneeded services, but only if one has an advanced technical knowledge of the OS. Included in the references are several links which highlight different services.[xix]

11. Teaching users how best to perform secure computing

Work with each user of the network. Explain the possible ways hackers can harm the family's equipment, personal information and finances. Teaching users how to use the Internet, email and network resources in ways which promote secure computing will go a long way in helping to maintain control of the network. Restrict users to certain actions if needed.

Parents need to sit with their children during chat room discussions. Explain to them what are appropriate statements and questions. Explain how to discern good conversations from threatening conversations. There may be resistance by children to have their parents interfere with chats and messages, but understand how serious the danger is out there. Sometimes adults just have to be firm and be a parent to their children rather than trying to be a buddy.

Teach all users in the household not to just inadvertently hit "OK" when a pop-up appears. Teach them to read what is

placed before them and to ask questions about what is presented on the screen. Included in the reference are some sites discussing safe computer usage for children.[xx]

12. Using company supplied equipment and policy for enterprise connectivity

Telecommuters need to work with their company's IT analyst to ensure they meet the necessary requirements established for home use of company assets. Strictly following the guidelines and procedures set by the company for their resources will help prevent malicious acts against the company. It may even save ones position in the company.

13. Using NAT

NAT is a Network and Transport layer translation technique. It allows publicly assigned IP address to be different from private IP address. This allows only the router to be "seen" from Internet hosts and not the computers. NAT is implemented by the perimeter firewall and should not be disabled. It is recommended to use private IP addresses in the internal network and implementing NAT via the firewall/router.[xxi]

14. Using encryption beyond the perimeter

Work with the ISP to ensure that clear text doesn't travel from home to the ISP. Using some form of encrypted protocol would need to be worked out with the ISP. The ISP will implement either SSL (Secure Sockets Layer) or IPSEC (Internet Protocol Security). Discuss with them what the options are for secure communication with their servers. There is more information on encryption in the references.[xxii]

Using the fourteen recommendations, the graphic design could then look like the one in Figure 2.

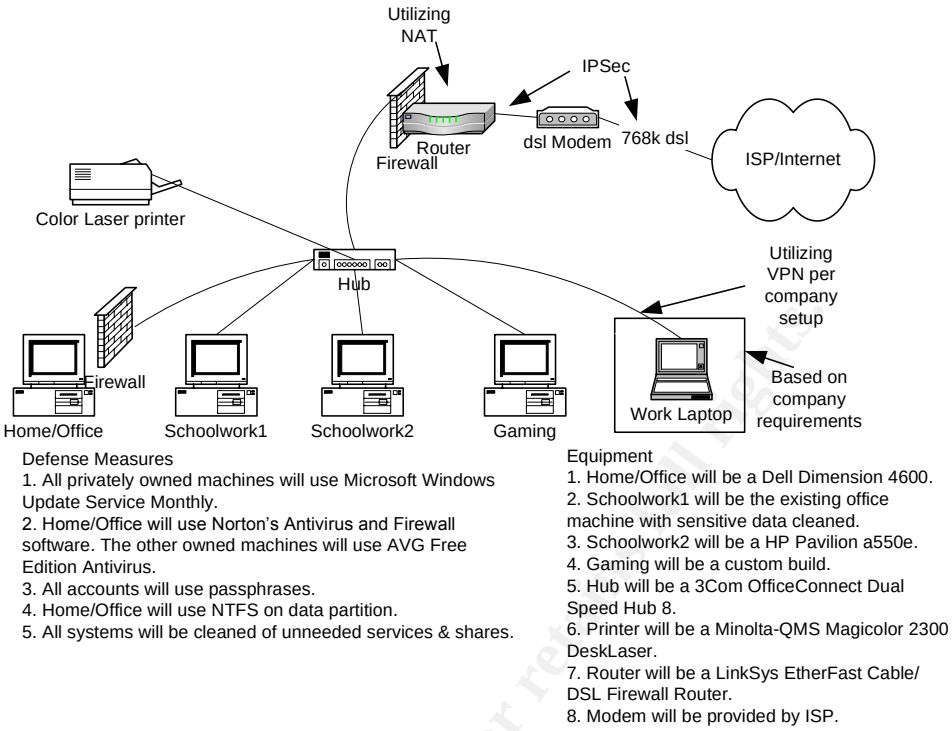

Figure 2: Secured Typical Network

Phase Four

Once the design is ready, it is time to begin the fourth phase which is purchasing. The buyer must be weary of purchases especially over the Internet. Don't be afraid to change the design slightly to accommodate good deals. After all, performance isn't a large issue in most homes, so if a deal is found on equipment that will work with the design then consider it. The number of possible places to purchase are too numerous; so research, research, research! Included in the references are a few sites to begin.[xxiii]

Phase Five

The fifth phase is building the network. Begin building with the most important and most sensitive resource in mind. If the home-office computer is the most important resource then begin there. Don't connect to the Internet until the network has incorporated a firewall. This is important!

Using Figure 2, set up the home/office computer first and then the perimeter firewall. Establish connectivity to the Internet and begin to pull down patches and update newly installed virus software. Next the

schoolwork computers and the game machine could be taken through the same process.

Phase Six

The sixth and last phase is to evaluate, baseline and document the network. Microsoft has a tool known as; Microsoft Baseline Security Analyzer (MBSA).[xxiv] This tool is easy to use and can help harden security. It is free to use as a service from Microsoft.

For XP machines, Security Configuration and Analysis Tool should be used.[xxv] It uses a created template to compare existing security against, so it is a bit more complicated. It is part of the XP OS as a MMC (Microsoft Management Console)[xxvi] snap-in. Learn how to use MMC first.

Once evaluation of the network is complete, baseline everything. This is accomplished through logs and backups. Using the auditing features[xxvii] create logs of the machines and then use these logs to periodically check for changes. Also by backing up the registry and system files at this stage of the build, there will be something to resort to which is known not to have malicious entities. Establishing a good schedule of backups and audits will only increase the chance of maintaining a secure network in the future. Documenting everything while things are still fresh will help later if there is a need to troubleshoot the network or if there is a change in the network.

Conclusion

The home user can't be allowed to stay in the dark. The self destructive path of uneducated home networking needs to be curtailed or eventually the cost to business and home users will become too great to continue the feasibility of having connectivity. The masses of individuals must be involved in the battle for Confidentiality, Integrity and Availability (CIA), commerce alone will not be able to maintain the fight.

More individuals that understand the ramifications of unsecured computing is the mission of this paper. It is not that secure computing is hard, it's just a matter of helping home users understand how to approach design and setup. There are numerous books, articles and web pages on home network design and security. If this paper is able to entice individuals to study and investigate how to properly establish and maintain secure home networks, then the mission is accomplished.

Summary

Hackers are real and they are plentiful. Understanding the threats, vulnerabilities and risks will help motivate individuals towards achieving secure networking. Without a large movement of typical home users working to secure networks, malicious code will grow in frequency and impact. The two greatest tools at the disposal of people are planning and research. This recommendation includes six phases: think about the requirements, research how to meet the requirements, design the network using Defense in Depth techniques, purchase equipment wisely, build the network logically and finally evaluate, baseline and document.

Reference:

[i] http://www.clickz.com/stats/big_picture/geographics/article.php/5911_151151 Article: Population Explosion! By ClickZ Stats Staff, May 10, 2004

[ii] http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/1060807172140_73?s_name=&no_ads= Story: Blaster Internet worm targets Microsoft systems, CTV.ca News Staff

[iii] Discussion: by James Robinson, Security Analyst; 4/30/2004

[iv] http://zork.net/~phil/Cracking/Internet.html Document: Phillip Dillinger; The Cracking Document

[v] http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A36498-2002Jul7&notFound=true Article: Internet Attacks On Companies Up 28 Percent, Report Says; By Michael Barbaro, Washington Post Staff Writer, Monday, July 8, 2002; Page E05

[vi] http://www.cnn.com/2001/TECH/internet/05/24/dos.study.idg/ Article: Study: Nearly 4,000 DoS attacks occur per week, By Sam Costello, CNN.Com/Sci-Tech

[vii] http://www.winnetmag.com/Articles/Index.cfm?ArticleID=42952&feed=rss&subj=WindowsSecurity Article: Spam Volume Reaches Record Levels; Paul Thurrott InstantDoc #42952, Paul Thurrott's WinInfo; June 10, 2004, Windows & .Net Magazine

[viii] http://www2.fmg.uva.nl/sociosite/websoc/pornography_child.html Paper: Child Pornography in Cyberspace, by Albert Benschop, University of Amsterdam, Department of Social & Behavioral Sciences

[ix] http://www.cert.org/tech_tips/home_networks.html Document: Home Network Security; CERT Coordination Center

http://secinf.net/ Network Security Library; WindowsSecurity.COM

http://www.sans.org/ The SANS Institute

http://www.interhack.net/pubs/network-security/ Paper: Introduction to Network Security, by Matt Curtin

http://www.microsoft.com/security/default.mspx Microsoft Security Home Page

[x] http://en.wikipedia.org/wiki/Operating_system Wikipedia The Free Encyclopedia

[xi] Discussion: by Matt Luallen, Instructor, February 2004

[xii] http://nsa2.www.conxion.com/support/guides/sd-1.pdf Guide: Defense in Depth.

http://www.computerworld.com/securitytopics/security/story/0,,93274,00.html?SKC=security-93274 Article: The defense-in-depth approach to malware, by Douglas Schweitzer; Computerworld

http://www.ebcvg.com/articles.php?id=219 Article: Defense in Depth, by Randy Stauber; eBCVG.com

http://securityresponse.symantec.com/avcenter/security/Content/security.articles/defense.in.depth.html Paper: Defense in Depth Benefits; Symantec Security Response

[xiii] http://v4.windowsupdate.microsoft.com/en/default.asp Microsoft Windows Update Site

[xiv] http://www.grisoft.com/us/us_dwnl_free.php AVG Antivirus Homepage

[xv] http://www.zonelabs.com/store/content/company/products/znalm/freeDownload.jsp Zone Labs, Inc.

[xvi] http://www.microsoft.com/technet/community/columns/cableguy/cg0204.mspx Microsoft TechNet

[xvii] http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/Default.asp?url=/resources/documentation/windows/xp/all/reskit/en-us/prkc_fil_duwx.asp Microsoft Document

http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/convertfat.mspx Microsoft TechNet

http://cws.internet.com/article/1470-1489.htm Tutorial: Should You Use NTFS? By Michael Hayman, WinPlanet Tips & Tutorials

[xviii] http://www.klcconsulting.net/Win2K_User_Mgmt.htm Article: Securing your Windows 2000, XP, and 2003 User Accounts and Passwords , by Kyle Lai; KLC Consulting, Inc.

http://www.microsoft.com/resources/documentation/WindowsServ/2003/datacenter/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/datacenter/proddocs/en-us/dsadmin_concepts_accounts.asp Microsoft Topic: Users and Computer Accounts

[xix] http://www.winnetmag.com/Windows/Article/ArticleID/40722/Windows_40722.html Article: Unneeded Services in Windows XP, by Michael Otey, Windows and .Net Magazine

http://www.mvps.org/winhelp2002/services.htm Article: Securing your Windows 2000, XP, and 2003 User Accounts and Passwords; MVPS.org

http://www.microsoft.com/technet/security/guidance/secmod54.mspx Guidance; System Services, Microsoft Technet

http://www.blackviper.com/WIN2K/servicecfg.htm Article: Windows 2000 Professional and Server Services Configuration 411; by Black Viper, BlackViper.com

[xx] http://www.ftc.gov/bcp/conline/edcams/infosecurity/forkids.html Site: For Kids; Federal Trade Commission – Consumer Information Security

http://www.solgen.gov.ab.ca/tips/children.aspx Site: Tips for Children; Government of Alberta – Solicitor General

http://safety.surferbeware.com/safe-computing.htm Ariticle: Safe Surfing; Surferbeware.com

http://familyinternet.about.com/cs/internetsafety1/a/safety01.htm Page: Family Internet - Internet Safety 101; by Marcy Zitz, About.com

[xxi] http://encyclopedia.thefreedictionary.com/Private%20IP%20address The FreeDictionary.Com

[xxii] http://www.google.com/search?hl=en&lr=&ie=UTF-8&oi=defmore&q=define:IPSec Definition: IPSEC; Google Search

http://www.google.com/search?hl=en&lr=&ie=UTF-8&oi=defmore&q=define:SSL Definition: SSL; Google Search

http://wp.netscape.com/security/techbriefs/ssl.html Article: Tech Brief-Secure Socket Layer; Netscape.com

http://www.winnetmag.com/Article/ArticleID/23446/23446.html Article: Using IPSec to Secure Communications; by John Howie, 12/17/2001, Windows & .Net Magazine Network

http://www.4d.com/docs/CMU/CMU02064.HTM Document: Using SSL Protocol; 4D.com

http://labmice.techtarget.com/networking/ipsec.htm Site: Windows 2000 IP Security (IPSec) Resources; Labmice.net

[xxiii] http://www.pricewatch.com/ Site: Pricewatch.com

http://www.streetprices.com/ Site: Streetprices.com

http://computerparts.addresses.com/category_search/Computer+Parts+and+Computer+Services/3/972.html Site: Computer Parts and Computer Services, Addresses.com

xxiv http://www.microsoft.com/technet/security/tools/mbsahome.mspx Tool: Microsoft Baseline Security Analyzer V1.2; Updated: February 20, 2004, Microsoft TechNet

xxv http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag_scmwhatis.mspx Document: Security Configuration and Analysis Overview

xxvi http://support.microsoft.com/?kbid=230263 Article: HOW TO: Create Custom MMC Snap-in Tools Using Microsoft Management Console; Microsoft Knowledge Base Article – 230263

xxvii http://support.microsoft.com/default.aspx?scid=kb;en-us;301640 Article: HOW TO: Set, View, Change, or Remove Auditing for a File or Folder in Windows 2000 ; Microsoft Knowledge Base Article – 301640

http://support.microsoft.com/default.aspx?scid=kb;en-us;300549 Article: HOW TO: Enable and Apply Security Auditing in Windows 2000; Microsoft Knowledge Base Article – 300549

http://support.microsoft.com/default.aspx?scid=kb;en-us;310399 Article: HOW TO: Audit User Access of Files, Folders, and Printers in Windows XP; Microsoft Knowledge Base Article – 310399

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS