Global Information Assurance Certification Paper

Richard Rodier
December 11, 2003

GIAC Security Essentials Certification
GSEC version 1.4B Option 2

LESSONS LEARNED FROM A WANNABE COMPUTER SECURITY SPECIALIST IN IMPLEMENTING A REALITY BASED HOME/SMALL BUSINESS COMPUTER SECURITY SYSTEM

Abstract

Home computer systems present a similar security concern, as do the corporate systems. As in the corporate world comprised home computer systems can be used by their captors to participate in Internet attacks on others. The loss of use or loss of data on a home computing system is an important concern. I have identified risks to my home computer environment. I then modified my home computing environment using skills learned in both the SANS class, on the job training, and experimentation. My goal was to implement concepts and methodologies specifically geared to be most effective, least expensive in both time and money, and easiest to implement. In the process of addressing this topic resources will be identified that would be useful in enhancing a home computing system.

Modification of my home computer environment focused on the following areas; network architecture and access; computer policy; operating system configuration; logs and intrusion detection; disaster recovery and home continuity plans.

Snapshot

The before environment included a teenager checking email on the internet using her mothers log on which had administrative access to her local computer with Windows 2000 Professional as the operating system. The network system had a cable modem provided by the cable company for access to the Internet. This went through one router with a hardware firewall with a standard configuration established by the manufacturer. Workstations included two Windows 2000 workstation, a Windows 2000 Server, one Windows XP professional workstation, and a Red Hat Linux Version 8 workstation.

Utilization of the manufacturer's standard out of the box configuration presented an enhanced risk of becoming compromised. All hardware remained in the configuration as the manufacturer shipped it and did not have the security features turned on. Lack of Policy management included no level of rights, and non-secure passwords. Log and intrusion detection was in remiss in that hard-ware firewalls and router did not have logging enabled. Disaster recovery and

home continuity area had limited backups and no plan for offsite storage of media or plan for evacuation.

Identified risks of home computer system prior to modifications

After consideration of the risk management section of The Cissp Prep Guide by Krutz and Vines[1], I chose the Qualitative Risk Analysis method to help identify and illustrate areas of concern related to the current state of my home computing environment. By using this method I did not have to associate financial amounts of money to a specific threat. Instead I was able to estimate the potential exposure of an item and assign a rating level based on the percentage of perceived loss. Course knowledge allowed the identification of the risks to my home computing system. The main risks were someone being able to take over the computer systems via administrative passwords, their installing of software compromising the security of the data and use of my computers. In addition to an active intruder there exists the potential for compromise of my systems from the everyday threats of emerging computer viruses. Other risks were loss of the computer systems themselves through failure of the hard drive, theft or accident. Systems could be compromised by malicious code or programs being installed on the computer systems by way of Internet browser issues related to weak overall security being an inherent part of the web browsers. In a Windows based operating system this is amplified by the fact that the web browser has been made an integral part of the operating system. I was able to rate the potential risks and found that several areas of my home computing model would provide a ripe environment for invasion. My teenager surfing the web, logged into my spouse's computer while using her log on which had administrative privileges was rated as a 100 percent loss of my overall computing systems. Short passwords were rated as potential 100 percent loss also. Standard configuration of routers and hardware firewalls were assigned a sixty percent loss potential. The router and hardware firewall appliance using the manufacturers default settings appeared to offer middle of the road protection. A forty percent rating was given for not providing potential added benefits by blocking industry-identified ports, which could be blocked. Default services running the operating systems had the potential to allow outside connections to control the computer system as well as potential use of mail servers and web servers. These issues presented several opportunities for improvement.

Operating systems were as offered by the manufacturer without taking security steps. No security auditing was taking place. The systems had several services running which could be exploited.
The lack of policy management presented an enhanced risk of becoming compromised such as no level of rights. With my teenager using the administrator account to surf the web the chances of the system being compromised was very real. The hardware firewall and router did not have

[1] Krutz and Vines p.15-25

logging enabled, and some of the features were not turned on by default. The manufactured default password had not been changed. The backups in place consisted of a monthly tape backup which would stay in the same room as the backup system. With the capacity limits of the tape media being close to full, it was difficult to capture all the data that needed to be backed up.

II. Implementation of system improvements

Modification of the operating Systems:

I have learned it is essential to strike a balance between extreme security, which would be very secure, but may also limit the utility of the systems. This learning experience was at times painful and frustrating as I applied higher levels of computer security to my home computing system. In experimenting with some of the tools described in this discussion one could easily eliminate almost all functionality of their computer systems. I used non-production machines to test my limits of acceptable utility and system security. I will focus on areas that I feel would provide the most return for the time and money invested for the protection of a home computer system. Douglas Ford published 8 Simple Rules For Securing Your Internal Network[2] providing information necessary to promote consideration of the areas and issues that I consider the back bone of the computer systems security model. Mr. Ford's work can be accessed by the Internet site http://www.sans.org/rr/papers/8/1254.pdf. I recommended any one interested in home or small business computer security become familiar with the eight rules identified by Mr. Ford. Mr. Ford states he and his penetration testing team are able to take ownership of some of their customer's domains in sixty seconds. This is yet another example of inadequately protected environments. The scary part is when a system is compromised the aggressor is most likely using someone else's computer, maybe yours or mine.

Red Hat Linux version 8 was installed on an older computer for my teenager to use. The deciding factor was that I felt the web browsers packaged with this software, would be less susceptible to the current web based exploits in the Internet environment. Any services not needed were turned off and the internal software firewall was enabled with the script I obtained from the Lab portion of my SANS Security Essentials Class. An important function of the script for me is that the system would not be seen and would not provide a response back to the scanning system. Given my limited background in managing and working with this operating system I opted to pay for the automated Red Hat system maintenance package. For a fee Red Hat will package the specific updates needed for your Red Hat Linux based system.

[2] Ford, p. 1-8

The system will visually advise me when updates are required. With a few clicks the update is completed. I configured the system with a root account and two administrator privilege accounts. Additional accounts were set up for general every day use with only basic permissions. I felt I had limited my exposure with a system that was easy to reformat as needed and be easily put back on line.

Most of the computer systems in my home environment are Windows based. I made initial adjustments by stopping or removing services I was not using. When Windows 2000 operating system is installed, a number of bells and whistles like a mail server or Internet web server may be installed automatically and started. These are all vulnerabilities if they are services that are not being used. The operating system configuration for Windows 2000 and Windows XP are different. There are many great resources available which can provide a path to follow to set the operating configuration as related to security issues. I prefer using guides published by the Operational Network Evaluations Division of the Systems and Network Attack Center (SNAC). These reports come directly from the National Security Agency (NSA), United States of America. As an example the NSA Report Number: C44-026-02 titled Guide to Securing Microsoft Windows XP http://www.nsa.gov/snac/winxp/guides/wxp-1.pdf by Bickel et al[3], covers all areas related to the security configuration of windows XP. It is best to have a machine to experiment on with the settings identified. If you are using your production computer keep an exact log of all changes made so they can be undone if you lose a specific functionality in the configuration process.

I experimented with two software firewalls for use on the windows operating systems. I used the Tiny Software firewall. On another system I installed the free version of Zone Alarm. The Tiny system is more robust having features found on more expensive firewalls. These addition options provide for enhanced port closure and filtering. I have concluded the Zone Alarm is better as it is easier to use. The Tiny has the superior ability but ease of use won out with the Zone Alarm. This is a good example of acceptable level of risk. With my defense in depth concept the less powerful firewall offers superior utility due to ease of use. I am willing to accept the increased risk exposure for the ease of use for my home systems. I do have strong feelings about the direction of the desktop, and notebook computer software firewall industry. Having worked in the computer industry with exposure to corporate, military, and educational server and desktop environments I have experienced the changes and worked with the tools made available by the anti-virus software companies. The advent of an anti-virus server capable of central management, synchronized updates, and the ability to install the anti-virus software remotely is in my opinion one of the best concepts put forth by the technology industry. It is with this background I am excited about the Tiny

[3] Bickel et al p.1-128

Software Company's[4] development of a product, which is a server for remote configuration, and management of their desktop software firewall program. A suite of three products is available, the above-mentioned Firewall Management Server, The Tiny Firewall Policy Editor, and the Tiny Personal Firewall 5.0 Enterprise. Information is available with via the following Internet link http://www.tinysoftware.com/home/tiny2?s=32293436685695557l6A0&offer=standard&pg=tfms_home. This concept is the greatest product since sliced bread offering great security benefits to a large home network, small business, or a large enterprise environment.

Another area, which is layered on top of the operating system, is the software. Specifically I would like to address configuration issues related to e-mail and the Internet explorer. *The NSA published a report* by Pitsenbarger and Bartock entitled E-Mail Security in the Wake of Recent Malicious Code Incidents[5]. http://www.nsa.gov/snac/emailexec/guides/eec-1.pdf. The authors state "Do Not attempt to implement any of the settings in this guide without first testing in a non-operational environment."[6] Unfortunately systems today are vulnerable to security problems. As time goes on manufactures will evolve from the we got to make it work mode to we got to make it safe mode. In the mean time it is up to us the end users to navigate through these configuration issues. This NSA E-mail security guide is twenty-two pages in length providing a solid base for configuration issues and addresses Microsoft Internet Explorer security zones.

Network Architecture and Access:

I used two types of routers with built in hardware firewalls. I started with a SMC 7004VBR Barricade router, which has state full packet inspection capability. The state full packet inspection ability makes it harder for a hacker to send in an unidentified packet string and have the router attempt to process it. With the state full packet inspection ability unidentified packets will be dropped. This router did not provide the option to block ports in a customized fashion.

The second router / firewall I used is a Linksys BEFSX41. I had a lot of fun with this, as I was able to modify access to incoming and out going ports with this model. The firewall logging options were superior to the SMC.

I eventually went back to the SMC after experiencing router-rebooting problems. I do not know if the traffic overwhelmed the machine or if the power supply was bad. I had installed the same Linksys for a friend and he experienced the same repeated rebooting of the Linksys router / firewall. The next step I took was to connect two SMC routers in series providing a sandbox type environment. The

[4] Tiny Software Company 2003
[5] Pitsenbarger and Bartock p.2-22
[6] Pitsenbarger and Bartock p.*2*

connection from my cable modem went to the first SMC, which generated a DHCP address to the second SMC. The second SMC then generated the DHCP address to my network and workstations. I eventually changed both SMC systems to hard coded IP addressing each with separate subnets. I disabled the DHCP as I saw it as a security risk. This was a risk of an outside intruder entering the system and obtaining a functioning IP address enabling spoofing opportunities. This was one more area I would not need to worry about. The original administrator passwords were changed to a separate individual one for each SMC router. The logging was turned on and each router was configured to send me e-mail if it sensed an attack. I removed a hub from behind the internal router and replaced it with a switch. This action eliminated the negative broadcasting and pass through behavior of the hub. The hub was retained for use with the intrusion detection system
Router configuration experimentation resulted in best balance of router configuration with minimal impairment of utility of system with given acceptable risk. Based on my experience with the above equipment, and the knowledge I have gained through my SANS education I would recommend the motivated home, or small business computer security manager (This is the new title people with computers on the internet, and with data to protect are whether they know it or not) invest in the Cisco Pix 501[7] Security Appliance. Cisco information is available via the Internet link http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/px501_ds.htm. The systems previously described are adequate however at a cost of under $600 it is possible to move to the next level of equipment using technology with a direct lineage to enterprise level security. One of the more exciting opportunities the equipment offers is the ability to make configuration changes as the threats change.

Computer Policy Implementation:

As in the corporate world policies are identified to create a good balance between acceptable levels of risk within acceptable levels of utility. Password type and management, email policies, user accounts and access rights will be shared.

Any users who would require administrative privileges on the systems such as mom and dad received two log in accounts, one with administrative privileges and one with standard user privileges for use in day to day daily computer such as writing documents, email and surfing the web. Password requirements were put into place with buy in of the importance of password policy. This required passwords in excess of fifteen characters. Users were advised that these passwords could be easily to remember phrases. They also were requested to have some upper case and numerals as well.

[7] Cisco Pix 501

Extensive policy configuration information for Windows 2000 operating systems is widely available. For my preference I again default to the Nation Security Agency, United States of America. The National Security Agency Operational Network Evaluations Division of the Systems and Network Attack Center (SNAC) Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set by J. Haney[8] can be accessed via the following internet address; http://www.nsa.gov/snac/win2k/guides/w2k-3.pdf. Mr. Haney provides a well-defined discussion on the Windows 2000 operating system group policy configuration options. The area I recognize as standing out is Chapter 9 Modifying File System Security Settings with Security Templates. In this chapter of nine pages Mr. Haney discusses permission options, which can be used on files and folders. Mr. Haney presents his own recommendations for settings adjusted and applied using the Microsoft Management Console Security Snap- in and the associated file folder template snap-in. The file system security settings area is one which I have had great difficulty, as in I took a well running system and made it useless. This is the part where I again recommend following the most basic of all recommendations for computer system professionals. Keep a configuration and change log history, and if possible make complete tests on a non-production system. I am not talking about the equipment at work because I know all computer systems professional would follow these practices, well maybe 99% of the time. It is the home system that these work standards need to be implemented. By employing the above tools provided by Mr. Haney and following basic configuration documentation procedures yet one more inexpensive, highly effective layer of security can be applied to the home computing systems.

Logs and Intrusion Detection:

I am a supporter of log reviews in an attempt to see if any one is borrowing the computer system. With the information overload the idea of a form of log reader or reporter is becoming commonplace. I can recommend two products both found at EventID. NET, somewhat costly, but not a lot as compared to some other systems. The first is Event ID[9] http://www.eventid.net/search.asp, which will provide a search on the web and at Microsoft for information on the specific event id, requested. This is helpful as some identified events are not harmful. When you identify an event and wish to explore the severity event id can help. A second product is Event Reader [10]http://www.eventid.net/eventreader/, which captures logs and makes a report out of them. This is helpful when trying to be diligent when caring for several machines.

I have found intrusion detection is best left up to SNORT. Snort is a freeware, which is complied into both Windows and Unix versions. Every thing you need to

[8] Haney p.81-94
[9] Event ID
[10] Event Reader

know and then some is available at the site http://www.snort.org[11]. I opted to use the windows version. On the Snort web site via the Internet web link http://www.snort.org/docs/snort-win2k.htm is a configuration paper titled Snort's Place in a Windows 2000 Environment written by John Bull[12]. This guide can help get you up and going with your own intrusion detection system. Additional help is available from the may Snort User Group[13] accessed on the Internet site http://www.snort.org/usergroups.html. By using the web site and accessing members of the user group I was able to learn about the Windows Operating System version of the Snort intrusion detection system. It was rewarding to have discovered this area to explore by way of my own investigation. When the topic of Snort was discussed in my SANS Security Essentials class I felt like I was finally getting ahead of the learning curve in the technology arena. This thrill quickly disappeared as other areas unknown to me were covered.

No home user should go for long periods of time with out utilizing the free security testing utility. This utility, provided by Mr. Gibson of Gibson Research[14] Corporation, maintains a business web site at the following address; http://www.grc.com. The utility is known as Leak Test[15]. To use this tool access the following site; http://www.grc.com/lt/leaktest.htm, follow the instructions and you will discover if malicious programs can access the internet from behind your firewall. This tool is especially helpful in the advent of the web-based methods hackers are utilizing to comprise our systems. This tool will help identify if you have a firewall that does what it is supposed to do, protect you.

Disaster Recovery and Home Continuity Plans:

In the corporate world the concept of business continuity covers a broad range of areas ranging from recovery computer system failures to recovery from local and regional disasters. Originally identified as Disaster Recovery a number of years ago the softer and broader identity of Business Continuity Planning is now common. Any one defending the position that computer security personnel need only be concerned with the back up of data and maybe keeping the data off site is misleading the people listening to them. I recommend attempting to identify all potential problems which might become an issue affecting the stability of your environment be identified and addressed. A formal business continuity plan would include not only the basic computer type stuff like backup and restore information, offsite storage, physical security and replacement equipment. The expanded scope would include thoughts on emergency contingency locations on a local and a regional level. Where do we go if the normal location is unavailable? Where do we go if the city we are in is unavailable? These are not

[11] Snort.org
[12] Bull
[13] Snort User Group
[14] Gibson Research Corporation
[15] Leak Test

unusual questions to ask. This is why corporate America has flowed with the various challenges presented in the past. The competition for funding to make the business continuity options available is in competition with other aspects of the environment. I anticipate more staff will be allocated by the corporate world to ensure the options that would be needed are identified and available when needed. Bob Miano authored an article entitled Key Considerations For Proactive Planning How to Mitigate the Effects of Disaster Prior to an Event[16]. Mr. Miano Identifies four key elements in his conclusion as follows; Less is more; Involve the recovery team, Distribution, and Testing. I have identified all four thoughts presented in the conclusion as being extremely note- worthy. First Mr. Miano presents a smaller better-understood plan is better than a cumbersome novel, which can be a turn off, and confusing to your team. The second suggests the author of the plan get very friendly with the staff to better understand the business process. In my own experiences I have seen the lack of understanding of a customers business model and work methods be a real showstopper. Mr. Miano goes on to note that every employee is part of the plan and should have their own physical copy. This will assist the employees in understanding what needs to be done, and how to do it. In the Testing portion Mr. Miano identifies an annual test schedule making room for any employee identified recommended modifications.

Now here comes our part. There is no reason the home environment cannot consider to a similar depth as the corporate world all the factors which would influence the home environment. The family home environments that experienced the wild fires of 2003 in California and the associated property losses set the stage for what is at stake. This discussion has not been made to tell the reader what to do or how to do it. I am sharing some of the thought process, which I consider and ponder in relation to my home computer security issues.

I will share one important, low cost, high security benefit value procedure. Send regular copies of your data, software license information, configuration logs, the preverbal important papers, and legal and financial information to a place far away on a regular basis. The far away and regular basis part is a variable in consideration of the risk and value of the possessions. Start asking questions and take to time to be aware of the speed negative situations can develop.

Home system after modification:

The final result was a teenager migrated to a red hat Linux system using an automatic updating service provided by the manufacturer. It allows for web browser, which would be more isolated from operating system vulnerabilities. Administrative and standard privileges were delegated; password requirements were put into place with a buy in of the importance of password policy. Network architecture work included blocking some incoming ports on the router, enabling logs for tracking purposed and installing two routers with hardware firewalls.

[16] Miano p.32

Software firewalls were implemented on the workstations. Switches as opposed to hubs were used for added security benefits. Operating system configuration changes resulted in turning off services not being used, and options providing for management of the computers outside the network environment were turned off as well. The windows configuration of SNORT provided a current reflection of any port scanning that might be taking place and any vulnerability, which the program helps to identify. The logs for the two different combination router and hardware firewall systems were captured and reviewed. In addition some basic logging systems were turned on to identify failed log on attempts and identify change of privileges. Disaster recovery in current status now includes a plan for retrieval of data in a remote location and an evacuation plan in the event of a local disaster. The thought process is started to identify options for housing for both short and long term needs that will support pets, family and provide for an area to house what possessions I may be able to bring.

References

Krutz, Ronald L & Vines, Russell Dean. The CISSP Prep Guide. Wiley. 2001. 15-25.

Ford, Douglas. 8 Simple Rules for Securing Your Internal Network. SANS Institute. Sept 2003. p. 1-8. http://www.sans.org/rr/papers/8/1254.pdf

Bickel, R.; Cook, M.; Haney, J.; Kerr, M.; Parker, T.; Parkes, H. Guide to Securing Microsoft Windows XP. National Security Agency. October 2002. http://www.nsa.gov/snac/winxp/guides/wxp-1.pdf

Tiny Software Corporation. Firewall Management Server, The Tiny Firewall Policy Editor, and the Tiny Personal Firewall 5.0 Enterprise. http://www.tinysoftware.com/home/tiny2?s=32293436685695557l6A0&offer=standard&pg=tfms_home

Pitsenbarger, Trent & Bartock, Paul. E-Mail Security in the Wake of Recent Malicious Code Incidents. January 2002. p.2-22. http://www.nsa.gov/snac/emailexec/guides/eec-1.pdf

Cisco Corporation. Cisco Pix 501. http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/px501_ds.htm

Haney, J. Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set. National Security Agency. December 2002. Version 1.2. 81-94. http://www.nsa.gov/snac/win2k/guides/w2k-3.pdf

Event ID.Net. Event ID. http://www.eventid.net/search.asp

Event ID.Net. Event Reader. http://www.eventid.net/eventreader/

Snort.org. Snort.org. http://www.snort.org

Bull, John. Snort's Place in a Windows 2000 Environment. Snort.Org. April 2002. http://www.snort.org/docs/snort-win2k.htm

Snort.org. Snort User Group. http://www.snort.org/usergroups.html

Gibson, Steve. Gibson Research Corporation. http://www.grc.com

Gibson Research Corp. Leak Test. http://www.grc.com/lt/leaktest.htm