Global Information Assurance Certification Paper

Derek Lawless

November 25, 2003

Securing and Auditing a Home Network

Abstract
This paper will seek to offer guidance and knowledge in securing and auditing a home network connected to the Internet with a high-speed connection for both basic and advanced users. In order to properly address the task, it will first explore the definition of a home network and the possible uses of a home network. The paper will then provide high-level security solutions to address a typical home network. Auditing of the home network will then be addressed. Finally the paper will touch on items to take into consideration in order to add future infrastructure without compromising the newly created security and audit infrastructure.

The Home LAN

According to the National Cable & Telecommunications Association (NCTA), the number of cable Internet customers has grown from just under 2 million in 2000 to nearly 13 million at the beginning of 2003. This huge jump in cable Internet use can be attributed to many things including utilization of the existing cable infrastructure, modest access charges, and increased speed over dial-up connections. In addition, computer price declines have allowed many homes to contain more than one computer. This has led users to begin linking the home's computers together into local area networks (LANs).

Home LAN Infrastructure

In general, LANs provide little security risk unless they are connected to the public via the Internet. Internal LANs with no connection to the outside world (video game LANs and data processing networks, for example) are easily controlled and need much less security than those connected to the Internet. For that reason, this paper will concentrate on home LANs that are connected to the Internet.

For the purposes of this paper, a home LAN will be defined as at least 2 computers connected to the internet on a fairly permanent basis through a hub, router, or switch. For home users that only have 1 computer connected directly to the Internet, many of the Internal Security controls will work, but the term 'home LAN' will not be used. As will be discussed later, connecting computers directly to the Internet is not recommended.

The most popular methods to connect to the Internet include cable Internet access, DSL Internet access, and dial-up access. Typical infrastructure required for high speed access is an access device such as a cable modem or DSL modem connected to a network interface card (NIC) in a computer or a network device such as a router, switch, or hub. Dial-up access requires an analog modem in the computer connected to an external phone line.

Users

The actual users of the home LAN make up an important component in not only the usage, but also the overall security of the LAN. The types of users, their

needs, and their knowledge all play important roles in setting up and securing a home LAN. Users can typically be broken down to several categories:

1. New users
2. Comfortable users
3. Experienced/knowledgeable users

Each user type has their own style of use and their own security risks that they bring to the LAN.

New users obviously have the lack of knowledge and comfort adding risk to the LAN. This causes them to make silly mistakes such as weak passwords, unmonitored downloading from the Internet, and opening un-trusted emails. These mistakes have the potential to bring in viruses and allow easier access for would-be hackers, but generally they don't create large scale security risks due to a fear of the technology. They rely on more experienced users to dictate their permissions and implement security practices.

Comfortable users generally pose the largest security risk. These users consider themselves to be knowledgeable enough to implement functionality such as web servers which can open large security holes if not properly secured. These users will often times introduce mitigating controls into their network but will fail to maintain them (i.e. Anti-virus software that hasn't been kept up to date). They may also "poke around" meaning they will change settings that they don't understand and fail to revert them. In addition to creating security holes, they could ultimately render the system or network unusable.

Experienced users are generally good choices for the home LAN administrators for obvious reasons; they are the most knowledgeable and many times have been burnt in the past by poor security controls. These users will incorporate mitigations such as keeping their virus definitions up to date, implementing personal firewalls, monitoring email attachments, and using strong passwords.

Each of these user types will be important to remember later when it becomes time to develop and design a security plan for the home LAN.

Network Functionality

In considering the best ways to secure a home network, it is also important to know what the purpose or main uses of the network will be. Knowledge of the purpose not only gives a greater understanding of the home LAN but also helps to draw out potential risks attributed to specific functionalities such as a home business. The common uses are often grouped as follows:

1. Home use only
2. External business access
3. Home business

Home Use only
Home use only would be described as a network used purely for use by the people in the home for leisure or home related activities. Surfing the Internet, checking email, and filing tax returns are all examples of common activities on a home use only network. This network is the simplest from an infrastructure perspective but may be the most complex from a user perspective due to the wide range of user groups.

External business access
This use would best be defined as one or more users accessing their business' network from their own home network; using a VPN client, for example, to connect to the internal network of their employer and perform work duties from their home. This usually does not require special consideration beyond home use only, however due to the possible sensitive traffic that could be traversing the network connection, encryption (via VPN most likely) is generally a requirement, not an option when connecting to the business network.

Home business
A home business is exactly that, a business, and should be considered as one when developing and designing the security for the home LAN. The variety of businesses that can be run from home is vast and thus the possibilities of the network's functionality are accordingly large. Typically, though, this use poses the greatest risk to the home LAN through the added functionality that must be secured. This may include web servers for e-commerce, mail servers for business email, FTP servers for file movement, and database systems for business data storage and processing. The challenge to this use involves providing adequate security controls without compromising business functionality.

Securing the network
The first step in creating a security plan for the home LAN is to perform an informal information risk assessment. This entails rating the sensitivity of any information contained on the systems inside the network and any information that will travel between internal computers and the Internet. This can be as simple as a personal importance value or as complex as a computed monetary value if information is lost or compromised. Obviously the importance of the information residing in the network will determine the level of security infrastructure. The network should be secured only to the point where the cost of the security controls is equal to the risk of loss or compromise of the data.

Securing Externally
The external side of the home LAN is the portion that the outside world sees. This entails the connection from the router, switch, or hub on the home LAN through the access device out to the ISPs border router. Any node on the Internet in the world can get to this device, since it has a routable IP address

provided by the ISP. This is the first point of defense that a home LAN has against the outside world.

As mentioned previous, the three pieces of network hardware most commonly connected to the access device are routers, switches, and hubs. Of those three, the hub is the most insecure. Hubs and switches are both essentially splitters for the signal coming in from the access device. They allow multiple computers to access the same outgoing network connection. The only difference between the two is that hubs will broadcast all traffic to all connections on them and switches will sort the traffic according to IP address. The two contain no mechanisms for security. Routers are slightly different in that they contain software which does the dispersing of packets to the correct IP addresses. This software allows them to contain ACLs which control the type of packets that can get through the router thus limiting who can connect through the router to the network inside.

Securing the router

Many home networks have small, cheap routers combined with switches to provide the gateway to the access device. The more popular models are manufactured by Linksys, Netgear, and D-Link. They run anywhere from $49 - $69 (Best Buy, 2003) for a 4-port model. These routers typically have an HTML web interface for configuring them. Figure 1 represents a Linksys router interface.

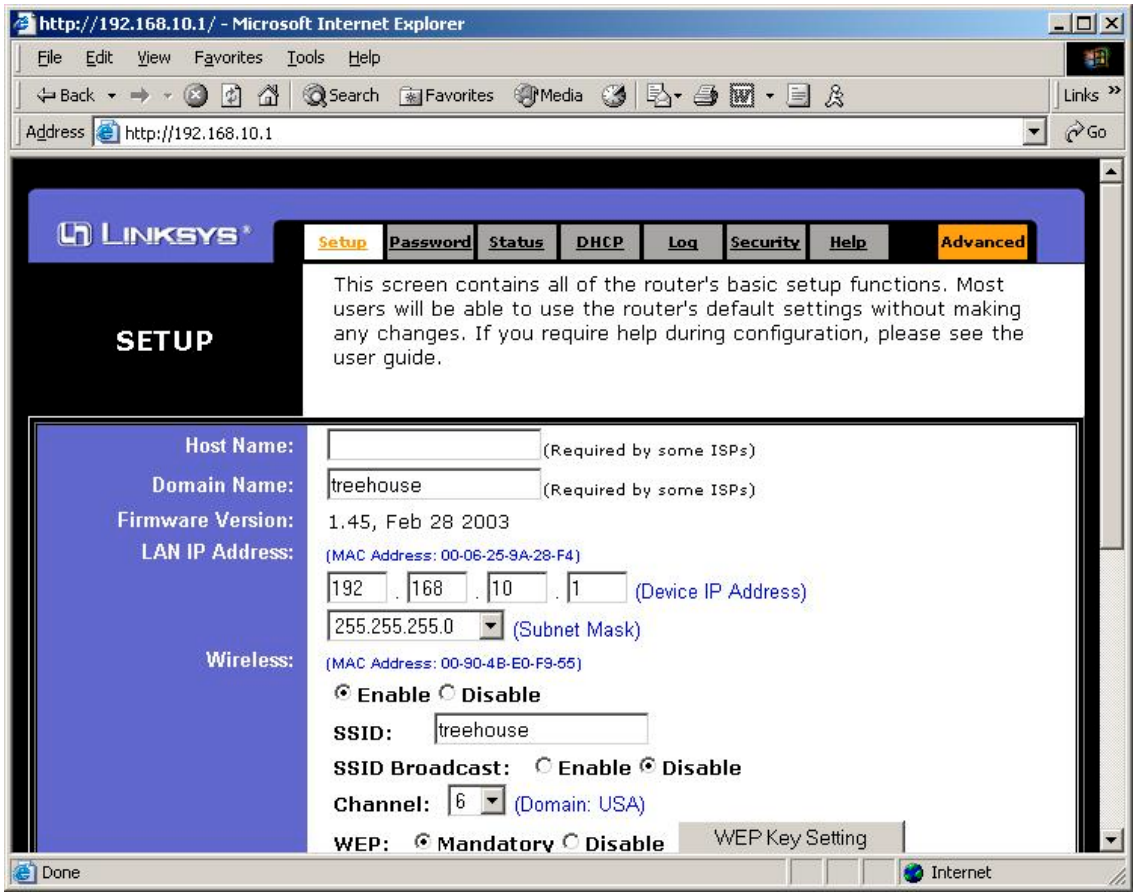

Figure 1

The best thing about these routers is that the out of the box configuration provides fairly good security. These routers use NAT to masquerade the entire home LAN behind one IP address. NAT was developed by Cisco to help alleviate the shortage of IPv4 addresses, but it also provides good security because the actual IP addresses of the internal network are hidden from the outside world. NAT works by using 1 address to represent an entire internal network. It takes a request from an internal computer to connect to an external address. It then takes the internal computer's IP address and source port and records it in the address translation table. The router then substitutes a unique port and the router's IP address in the outgoing packets. When a reply comes back, the router looks to the address translation table to resolve which internal computer the traffic should get routed to. This configuration ensures that packets from external hosts that did not have a connection established are not routed. If packets from the outside cannot get in without a connection initiated by one of the internal computers, the bad guy's job has become much more difficult; hopefully difficult enough to deter any would be hackers.

An important note on routers, such as the Linksys BEFSR11 EtherFast® Cable/DSL Router, is that they come preconfigured with a default administrator's password. These passwords are the same on all Linksys BEFSR11 routers.

The manufacturers know this, end users know this, and of course attackers know this. The first thing to do after purchasing the router is to change this password to something secure. Usually something with 8 or more characters made up of numbers, upper and lower case letters, and special characters is appropriate. This password is important. It literally is the key to the front door. Another important step to perform immediately after setting up the router would be to upgrade the firmware. The firmware is basically the operating system of the router. The router usually ships with the first version of the firmware developed for that particular model of router. Over time, as with all systems, vulnerabilities are found and fixed in subsequent releases of the firmware. The router interface should have an upgrade function that will allow the user an easy means of upgrading. Check the help documentation for the router and the vendor's support website for exact directions on upgrading the firmware.

Securing Internally

Internal security is a very important aspect that is sometimes overlooked. Having a router or firewall on the outside is no doubt very important, however if an internal user requests something bad from the outside, the router or firewall will likely allow it through. An example of this would be a virus attached to an email. The nature of an internal network is that there is an elevated level of trust between computers on the internal side of the router. This further increases the risk of compromised computers attacking each other successfully.

Anti-Virus Software

The most common security software on personal computers is undoubtedly anti-virus software. The most popular anti-virus software in use today is Symantec's Norton Anti-Virus™. Other popular brands are McAfee and Command. Anti-virus software compares signature files created by the anti-virus companies to all the files on the computer looking for matches in script files, binaries, and email messages. Anti-virus software is important to all systems, particularly ones which will have new users. New users, as mentioned before, tend to take security for granted and will open email attachments which could contain viruses. For this reason, it is important that the home LAN administrator install anti-virus software on all systems and keep the virus definitions up to date.

Personal Firewalls

Personal firewalls are application-layer firewalls that are installed on the computers of the home LAN. Application-layer firewalls work between the application and transport layers of the Internet Network Model. They prevent applications from accessing the network unless the firewall's rules allow. They also prevent incoming connections from accessing the system without specific allowance from the firewall rules. If properly configured, the firewall will appear invisible to end users. This is helpful to keep new users from being scared by firewall messages.

Operating Systems

One of the most important components of the home LAN is the operating systems that run on the computers. The operating system's own defense is typically the last line against attackers who wish to gain control of the OS for malicious activity. Securing it against unauthorized external access, as well as internal access, is imperative to maintaining a secure home LAN.

The majority of home computers run some variant of the Microsoft Windows® operating system. There are different versions and each has varying layers of naturally built in security. Newer versions tend to have greater security built into "out of the box" installs than older versions. Even the most recent versions, however, aren't incredibly secure without some configuration. "Out of almost 30,000 successful attacks recorded by mi2g Ltd. this year so far, 47 percent were on systems running Windows…" (vnunet.com, 2003).

No matter the operating system, the key home LAN security controls are the same. One of the most important is to use strong passwords on all user accounts. Poor passwords are easy to crack with modern cracking tools and they are the first step into the OS from attackers. Another important OS security control is file ACLs. These access control lists define who can perform the various file actions such as read, write, and delete. By removing anonymous accounts such as *Everyone*, and eliminating unnecessary permissions from other users, sensitive data and system files can be protected from unauthorized access.

It is also very important that the home LAN admin keep the OS system files up to date. This involves applying hot fixes and service packs as they are released from the vendor. Many security breaches occur months after a hot fix for the vulnerability is released.

Remember that the OS must be able to remain usable. If users cannot do the things they need to do, they will not be happy and this can lead to security issues down the road from disgruntled users. Give users all the accesses they need, but only the accesses they need. Keep administrative access to a minimum and perform day to day work with a non-administrative account. This can prevent malicious code from running rampant across the system with full access.

Miscellaneous Infrastructure

In addition to the usual home LAN infrastructure, there are a few special, less common pieces that should also be touched upon. These special cases are most commonly used in a home business situation and should be implemented only if explicitly needed.

The most common addition to the home LAN that is out of the ordinary is the web server. Web servers allow web content to be published for internal and external users to browse. In the case of e-business, they would be primarily directed toward external Internet users. This obviously introduces another doorway for

potential attackers to exploit. In order for HTTP to operate and transport content to end users, an additional port must be opened on the operating system to allow incoming connections. Nearly 70 percent of attacks in the first quarter of 2002 used port 80, the port commonly used for HTTP (IT Week, 2002).

If a web server is absolutely necessary for the home LAN, care should be taken to secure it properly. This involves keeping the OS security for the server up to date and keeping the server segregated from other servers on the network. This can be done by keeping the server in a DMZ. Many of the common routers, such as the Linksys BEFSR11 mentioned in this paper, provide DMZ functionality. By designating the web server to be part of the DMZ, the rest of the network is protected in the event that the web server is compromised. The only port that should be opened to the outside world would be the HTTP port. All other ports should be closed to external connections to lower the risk of compromise. In addition, the web server software should be secured using a tool such as the IIS Lockdown Tool from Microsoft, designed for use with Microsoft IIS® web server.

Additional web server security controls are web server software specific and outside the scope of this paper. Users are recommended to exercise extreme caution and urged to research securing the web server and platform for a successful and safe deployment.

Limitations

In an ideal world, all systems would have the maximum amount of controls available to secure the infrastructure. Unfortunately, many limitations prevent this level of security from being implemented, particularly in the home sector. Security systems and controls often incur additional cost to basic home computing systems. This may include purchasing routers/firewalls, anti-virus software, and more secure operating systems.

Time is another important constraint. Often times, home LANs are hobbies of people who have full time jobs and are using their free time to implement the network. The time required to implement and monitor extensive security controls can outweigh the actual benefit from having these extensive controls in place. Balance between time spent and level of security ensures that enough security controls are implemented but excessive, unmanageable controls are left out.

Auditing

According to the Microsoft Corporation, auditing is the process of tracking security-related events that occur on a system. These invents include creation, modification, deletion, and access of files, folders, services, or accounts. These activities can tell a detailed story of the activities users and programs are performing.

Footprints in the sand

The goal of auditing is to track activities, formulate patterns, and provide insight into the activities of the system so that unauthorized activities and accesses can be prevented or unwanted consequences can be reversed. Each action a user or program takes on a system is a potential "footprint." Experienced intruders know that the key to escaping detection is to attempt to erase these footprints. Often times, however, the act of erasing the footprints may cause more footprints.

Innocent vs. malicious activity

Searching through the log files of a system can, to use an old cliché, often be like searching for a needle in a haystack. The amount of information a log contains is often large and sometimes incomprehensible to the untrained eye. The key is to look for odd activity. By using patterns in the data, innocent, common data can be discerned from potential breaches and malicious activity. After all, finding the malicious activity is the goal of a security audit in the first place.

Simple Auditing

Home users can do a great deal of simple auditing without fancy techniques or expensive auditing tools. Successful auditing of a home LAN relies on the user's knowledge of the systems on the LAN and all the applications, information, and settings that are contained in those systems. Many security breaches are often stumbled upon when a user notices something out of the ordinary on the system. Missing data, strange access times, new or modified files and applications, and loss of functionality are a few obvious signs that the home LAN may have been compromised.

Simple auditing requires the administrator or maintainer of the network to have a reasonably good idea of the usage habits of authenticated users on the network. This will help with the "needle in the haystack" search for malicious activity.

Simple auditing techniques, as discussed above, should be an almost unconscious part of the home LAN security methodology. Responsible administrators and even responsible users should maintain a high level of awareness to any changes or unexpected activity on their systems, user accounts, and data.

Advanced/Custom Auditing

This topic is reserved primarily for the paranoid breed of home administrator. These individuals feel that either the information contained in their home network is of a high sensitivity or are interested (perhaps even a little obsessed) in security and desire to keep a firm handle on the state of their home LAN. Under normal conditions, with proper mitigating controls such as firewalls and NAT routers in place, home LANs are fairly secure to outsiders. However as stated above, if a home business is on the network or other sensitive data is stored inside the network, advanced auditing techniques may be necessary to ensure proper security and mitigate risk of data loss, corruption, or unauthorized access.

Most operating systems and network routers/firewalls incorporate auditing controls which can allow observant and knowledgeable users to remain informed of the status of their systems. A good example of advanced logging is Microsoft Windows® Event Viewer. Event Viewer contains a security log which can be configured to capture many types of security events such as logons, file access, account management, privileged use, and several others. Figure 2 shows the Event Viewer security log.

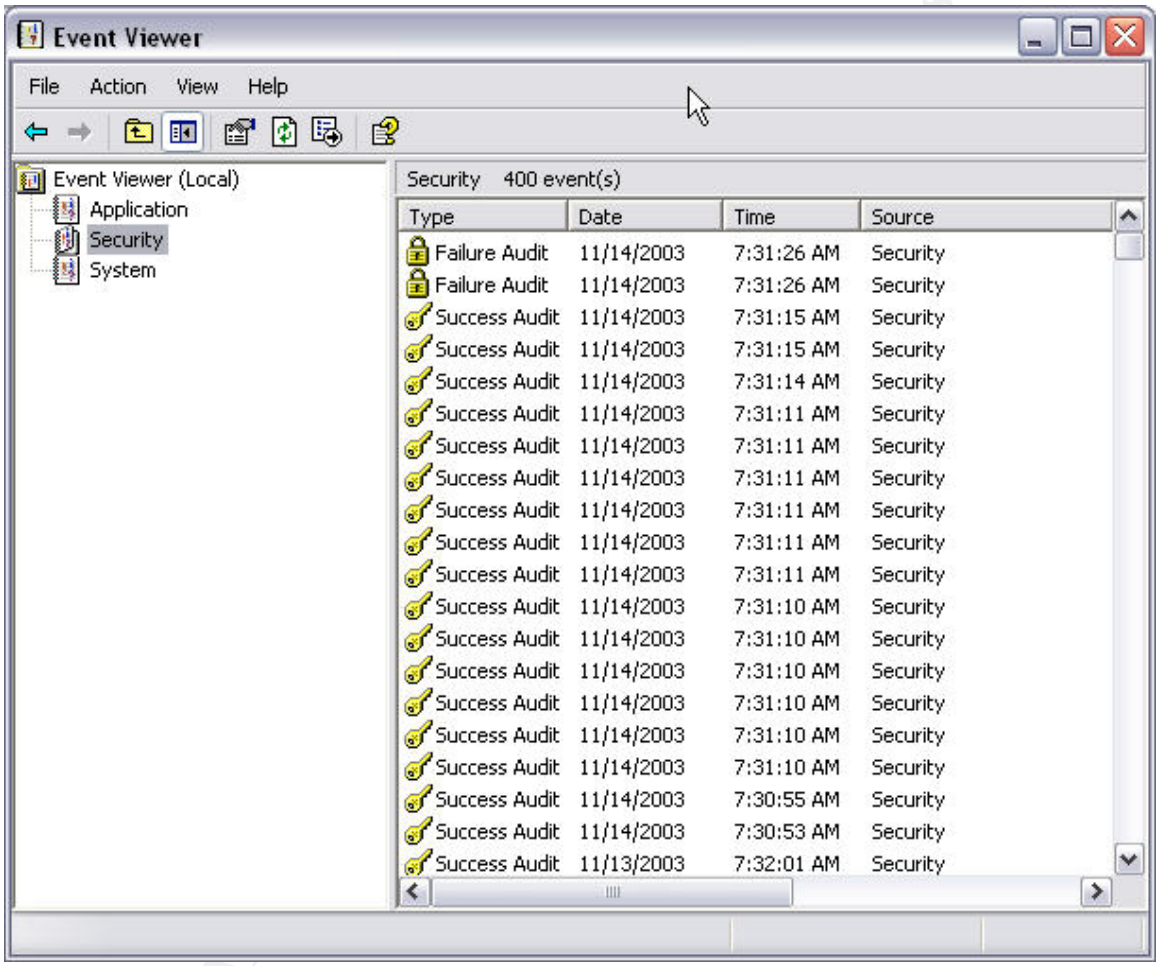

Figure 2

The log will capture successful, failed, or both types of events. The types of events audited are configured using local security policy for standalone computers or group policy objects for Windows domain computers. Configuring these policies is outside the scope of this paper but Microsoft has excellent documentation on configuring Windows 2000 and Windows XP security policies to capture the desired events at http://www.microsoft.com/windows2000/techinfo/planning/security/entsecsteps.asp.

Even relatively inexpensive routers such as the Linksys BEFSR11, contain auditing functionality to track incoming (from the Internet) and outgoing (from the internal LAN) connection attempts. Linksys provides an application, LogViewer, which will retrieve the log file from the router and bring it to a computer specified on the router interface. This allows an administrator to audit attempted access to the internal network from Internet addresses. The destination port number, source port number, destination address, time, and source address are all recorded.

LogViewer basically just dumps all the access attempts from the router to a text file. Often these files can become very large in the matter of only a few days. A custom tool can easily be crafted to search through the log file and pull out only the information of interest to the administrator and sort it in any desirable fashion. Included in this paper is an author written tool in Perl that will take LogViewer logs and parse them to two separate files. One file contains log entries sorted by destination port number and the other contains entries sorted by source IP address. The purpose of the first is to monitor ports with known attacks and vulnerabilities (80, 135, 1434, etc.) and the second to monitor who is attempting to connect. Not all attempts are malicious, however multiple attempts from a single unknown IP can be a cause for further monitoring. Figure 3 shows the sample output sorted by source address and Figure 4 shows the sample output sorted by port.

Figure 3

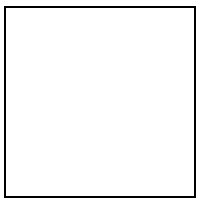

Figure 4

Adding future infrastructure

It would be naive to assume that a home LAN would never change. It is important to consider changes to the LAN thoroughly before implementing them as they could have adverse effects on the security controls that are already in place. Every change to the environment is important because something as little as a new software program could compromise the security already in place. It is also important to research changes because current security could prevent the new infrastructure from performing properly. As infrastructure becomes obsolete, it is important to replace security controls that the old infrastructure provided with new infrastructure or restructured security controls.

In addition to considerations for new infrastructure, new vulnerabilities and exploits released for current infrastructure should always be monitored so that any potential breaches can be mitigated as they become available. This is essential to maintaining the health of the home LAN and its security controls.

Conclusion

Familiarity and knowledge of the home LAN are the administrator's best tools for securing it. Keeping a constant and up-to-date understanding of all the systems, users, network infrastructure, information, and uses of the network will simplify auditing, ease infrastructure additions, and ensure that security controls are current and sufficient. Knowledge of the latest vulnerabilities for the infrastructure incorporated into the home LAN will enable proactive responses and fixes. Audits should be conducted on a regular interval to maintain the knowledge of the home LAN and to protect its resources.

The following checklist is a basic set of security controls to incorporate into a home LAN:

- Install a router/firewall that does NAT to protect internal systems
- Change the administrator password for the NAT router/firewall
- Upgrade the router/firewall firmware to the latest version
- Install anti-virus software on all internal systems
- Download the latest anti-virus definitions
- Install all of the latest hot fixes and service packs for operating systems
- Install personal firewalls such as ZoneAlarm on internal systems and configure them to block all uninitiated incoming connection attempts
- Remove *Everyone* group from all ACLs on folders on Microsoft Windows®
- Limit the use of administrator accounts to only administrative tasks

This list is by no means an all exclusive list. Let the infrastructure dictate exactly what security controls to incorporate. Knowledge and proactive actions are the weapons and with them a home LAN can be as secure as the largest corporate network.

Acronyms

ACL *– Access Control List*
DMZ *– De-militarized Zone*
DSL *– Digital Subscriber Line*
FTP *– File Transfer Protocol*
HTTP *– Hypertext Transfer Protocol*
IIS *– Internet Information Services*
IP *– Internet Protocol*
IPv4 *– Internet Protocol version 4*
ISP *– Internet Service Provider*
LAN *– Local Area Network*
NAT *– Network Address Translation*

OS *– Operating System*
VPN *– Virtual Private Network*

Source code

```
#!C:\perl\bin\perl.exe

# logviewer_report.pl
#
# Created by: Derek Lawless
# Date:       7/6/2003
#
# This program will parse a Linksys LogViewer log file to
# create reports on incoming traffic trends.
#
# Incoming logfile is named "Incoming.log"
#
# Output will be written to files called "ip_report.txt" and
# "port_report.txt"
#
# Incoming logfile input lines in the form of:
# mm/dd/yyyy hh:mm:ss Incoming_IP Incoming_Port# Destination_IP
Dest_Port#
#

use strict;
# Preprocessing work #
my ($sec,$min,$hour,$mday,$mon,$year,$wday,$yday,$isdst) =
localtime(time);

# Numeric Sort #
sub numerically {$a <=> $b;}

# Initialize filehandles #
open(IN, "Incoming.log") or die "Can't open logfile!";
open(IP, ">ip_report.txt") or die "Can't open ip report file!";
open(PORT, ">port_report.txt") or die "Can't open port report file!";

my $line;
my %by_ip;
my %by_port;
my $item;
my $index;

while($line = <IN>)
{
   if(substr($line, -1, 1) eq "\r"){chop $line;}
   if($line =~ /^(([0-9\/]+)\s+([0-9:]+)\s+([0-9\.]+)\s+([0-9]+)\s+([0-
                9\.]+)\s+([0-9]+))/)
   {
      push @{$by_ip{$4}}, $1;
      push @{$by_port{$7}}, $1;
   }
}

#=====Sorted by IP======#
print IP "Report sorted by Source IP Address\n";
print IP "---------------------------------\n";
```

```
foreach $item (keys %by_ip)
{
   print IP "    Attempts by: $item\n    -----------------\n";
   foreach $index (0.. $#{$by_ip{$item}})
   {
      print IP "    $by_ip{$item}[$index]\n";
   }
   print IP "\n";
}
#=====Sorted by Port====#
print PORT "Report sorted by Port Number\n";
print PORT "--------------------------------\n";

my $a, $b;

foreach $item (sort numerically keys %by_port)
{
   print PORT "    Attempts on port: $item\n    -----------------\n";
   foreach $index (0.. $#{$by_port{$item}})
   {
      print PORT "    $by_port{$item}[$index]\n";
   }
   print PORT "\n";
}
$mon++;
$year += 1900;
print PORT "\nReport complete $mon\/$mday\/$year $hour:$min:$sec\n";
print IP "\nReport complete $mon\/$mday\/$year $hour:$min:$sec\n";

# Cleanup file handles #
close IP;
close PORT;
close IN;
```

References

"About Symantec – Corporate Information." URL: http://www.symantec.com/corporate (25 November 2003).

Franklin, Curt. "How DSL Works." How Stuff Works. URL: http://electronics.howstuffworks.com/dsl.htm (25 November 2003).

Franklin, Curt. "How Routers Work." How Stuff Works. URL: http://computer.howstuffworks.com/router2.htm (25 November 2003).

Geralds, John. "Web-based attacks set to soar." ITWeek.com. 05 April 2002. URL: http://www.itweek.co.uk/News/1130673 (25 November 2003).

"History of the Internet." 1997. URL: http://www.msichicago.org/scrapbook/scrapbook_exhibits/commex/history.html (25 November 2003).

"Home Network Security." Cert Coordination Center. 5 December 2001. URL: http://www.cert.org/tech_tips/home_networks.html (25 November 2003).

"How NAT Works." URL: http://www.cisco.com/warp/public/556/nat-cisco.shtml (25 November 2003).

"Linksys BEFSR11 EtherFast® Cable/DSL Router." URL: http://www.linksys.com/products/product.asp?grid=34&scid=29&prid=142 (25 November 2003).

"Microsoft TechNet Glossary." URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/gl_glossary.asp (25 November 2003).

Middleton, James. "Windows hack attacks on the rise." Vnunet.com. 16 August 2002. URL: http://www.vnunet.com/News/1134436 (25 November 2003).

"National Cable and Telecommunications Associaton – Broadband Services." 30 June 2003. URL: http://www.ncta.com/Docs/PageContent.cfm?pageID=93 (25 November 2003).

"Step by Step Guide to Configuring Enterprise Security Policies." URL: http://www.microsoft.com/windows2000/techinfo/planning/security/entsecsteps.asp (25 November 2003).

Thomas, Kim. “Building a Secure Home Network.” GSEC Reading Room. 26 July 2001. URL: http://www.sans.org/rr/papers/index.php?id=611 (25 November 2003).