Global Information Assurance Certification Paper

Computer Security Outside the Company Walls
By David J. McCune
Assignment version: 1.2f

Corporate-level computer security has gained worldwide attention over the last two decades, but most home computer users still believe they are not at risk. When home computer users do not manage a web site or save corporate secrets on their home computers, they believe they couldn't possibly be in jeopardy of becoming a victim to crackers. For years now, corporations and non-profit organizations alike have been spending large amounts of money to protect the availability, integrity, and confidentiality of their information through the use of firewalls, intrusion detection systems, sniffers, and vulnerability scanners. Home users, however, are usually equipped with nothing more than virus protection, saying, "It's just my home computer; isn't that enough?" Not anymore.

DSL lines in service in the United States totaled 3,821,640 at the end of third quarter 2001 ("North America," 2001). These statistics were published by Telecom, Inc. and showed an increase from "504,100 DSL lines [in the U.S.] in service at year-end 1999" ("North America," 2000). This astounding increase in broadband technology encompasses only the DSL market, not the thousands of home users with "always-on" cable modems. The resulting problem is candidly stated by Adam Cohen in Time Magazine, "These 'always on' connections are catnip to crackers because they are stationary targets, vulnerable to attack 24 hours a day." With the dramatic increase of the "always-on" Internet and the lack of consumer education regarding security concerns, most home computer users have unknowingly opened a front door to their computer and their computer files.

"Always-on" home Internet connections have provided a growing venue for crackers. But what would they want with *your* computer? Many intrusions are harmless. These intruders simply want to see if they *can* gain access, similar to a teenager seeing the keys in your car and taking it for a joyride in the middle of the night. Sure, accidents happen, but that wasn't the intent. Identifying vulnerabilities on your home computer and exploiting those vulnerabilities to remotely access your files may be done for mere bragging rights, but other intruders are not so "innocent." Some of them are looking for your credit card numbers, your bank account information, or corporate information brought home from work. A cracker could even use the open-access to your home computer for a larger purpose: to launch a Denial of Service (DoS) attack. In this event, a cracker users your computer as one source of incoming information to a larger network. By using your computer with others' computers, the larger network is bombarded with information and ultimately crashes. Do you want to be partially responsible for an attack on another person or persons' system?

Many home computer users assume the above examples are extreme cases. They are not. I am an average computer user who lives in a fairly rural area. After choosing a firewall and installing it on my home computer, I had an immediate port probe reported from my firewall software. Anymore, reports of blocked scans and probes are a routine occurrence whenever I'm connected to the Internet.
What should be in place and protecting the home computer as well as the rest of the home network are some of the same tools and procedures used in the work environment:

- a well configured firewall
- an intrusion detection system
- periodic use of a vulnerability scanner
- routinely updated virus protection
- periodic back up of the data stored on the computer

Personal Firewall

A personal firewall is software or hardware that monitors events and either denies or allows outgoing traffic known as egress filtering or incoming traffic known as ingress filtering. A firewall should be the first line of defense in protecting the availability, integrity, and confidentiality of data in the home computing environment. While a company may use packet-filtering routers for perimeter defense and host-based firewalls as an additional line of defense, in the home environment, the personal firewall plays a key role by defending the network and individual host perimeters. Several commercial and freeware versions of personal firewalls are available on the market. The commercially available versions can cost between $40 and $200 and include Net Ice's Black Ice Defender, Norton's Personal Firewall, McAfees's Firewall, and Zone Alarm Pro 2.6. Some freely available personal firewalls are Zone Alarm version 2, Tiny Personal Firewall version 2, and Sygate version 4. Each of these firewalls can be downloaded from the following web sites respectively:

Black Ice Defender: http://www.networkice.com
Norton's Personal firewall: http://www.symantec.com
McAfee's Firewall: http://www.mcafee.com
Zone Alarm (both commercial and free version): http://www.zonelabs.com
Tiny Personal Firewall: http://www.tinysoftware.com
Sygate: http://www.sygate.com

No matter what personal firewall a home user decides to run on his system, he must take the time to configure the firewall correctly. This does not take extensive computer training. Depending on how involved the user wants to get, configuration can range from making simple decisions of when the intrusion detection system alerts to editing specific command lines in the firewall code to block connectivity to specific IP addresses. Following the software's manual, help files, or online tutorial can help in understanding the basic settings. Whether the user chooses simplicity and possibly less security or advanced configurations with stronger security settings, he or she needs to be aware of the different operations running on the system so normal and abnormal events can be recognized. As stated in the SANS Security Essentials Manual titled Network Security, "An event is any observable occurrence in a system and/or network" (SANS, 2001). Events are not necessarily bad or malicious in nature; a file being deleted from a computer by a user is a normal event. However, an event is malicious in nature when a virus or Trojan causes the same file to be deleted, sends the file to another user, or modifies the data in the file all without the user's knowledge.

When alerting activity message boxes begin popping up, the user needs to be able to make an informed decision as to whether the events are legitimate and should be allowed to continue, or incidences and should be looked at more closely. The user normally has many choices as to what permissions will be assigned to the questionable activity: block activity permanently, block activity for a specified amount of time, allow activity for a specified amount of time, or allow

activity permanently. I find it reassuring to know that because of my personal firewall no software can connect to the Internet without my explicit permission. I have complete control over how my computer operates.

To see an informative evaluation of some commercially available and freeware firewalls go to Sean Boran's article titled, "An Analysis of Mini-firewalls for Windows Users" at http://www.boran.com/security/sp/pf/pf_main20001023.html.

Intrusion Detection System

The next line of defense in securing the home computing environment is an intrusion detection system. An intrusion detection system will not prevent someone from entering your cyber world, but it will notify you of suspicious activity on communications ports. Obvious activity can appear as specific types of Trojan port scans such as Satan, Netbus, and Subseven port scans. However, this activity may not be so obvious when the user has unknowingly executed a Trojan on a computer, giving a cracker access without the user's knowledge.

More and more firewall programs are coming with intrusion detection built in. Two such programs are Black Ice Defender and Zone Alarm. These types of intrusion detection systems will identify suspicious activity and alert the user with pop up windows and different logging options. The user then has the option of creating or adjusting permissions for activity. Intrusion detection systems can provide the user with valuable information such as the threats that are reaching the user's computer. Receiving notifications from an intrusion detection system that a computer is consistently being scanned could be the information needed to adjust security settings in the firewall before a cracker is able to gain access.

If a cracker is able to bypass the firewall's defenses, the intrusion detection system is there to alert the operator. This gives the operator an opportunity to adjust the settings to his or her firewall, possibly preventing attacks of the same type in the future. Microsoft has built useful intrusion detection tools into its operating systems. One such tool is Netstat. Netstat is a DOS program that, when executed, displays the status of each communications port, such as whether the port is established or listening. To execute Netstat, the user can type "netstat –an" from the DOS prompt. This will display basic communication port information.

In order to utilize Netstat, the person viewing the information must have a basic understanding of what is being displayed.

- The first column lists the type of communication protocol being used such as Transmission Control Protocol (TCP) or User Datagram Protocol (UDP).
- The second column lists the local IP address port number.
- The third column lists any foreign IP address that may be talking to the local address.
- The fourth column lists the state of the local address such as whether the local address is listening or communicating with a foreign address.

From a security standpoint, this information is very important because it will tell the operator how the computer is attempting to talk to other computers (whether the operator has authorized the connection or not). Certain Trojans are notorious for utilizing specific ports on attacked

systems in an attempt to establish a link with a cracker. Three of the more notorious Trojans and their default ports are Sub-Seven (ports 1243, 6711-6713 6776, 16959, 27374, and 27573), BackOrfice (ports 1349, 8787, 8879, 54320, and 54321), and NetBus (ports 12345, 12346, 12456, and 20034) (DoSHelp, 2001)

Memorizing ports do not have to be the home user's priority. If your system reports a suspicious port, these two web sites are available to help interpret the information provided by Netstat: http://www.iana.org/assignments/port-numbers and http://doshelp.com/trojanports.htm. The first web site belongs to the Internet Assigned Numbers Authority and lists all assigned ports and what programs/operations should be using a specific port. The second web site belongs to the Intrusion and Attack Reporting Center and provides an extensive listing of attacks against computers and what ports are normally used to capitalize on the attack. The Center for Internet Security also has a list of common vulnerability ports. This list can be obtained at http://www.cisecurity.org and is titled, "Appendix A-Common Vulnerability Ports."

Another piece of the intrusion detection model for home users who do have security sensitive files is an integrity checker such as Tripwire, available at http://www.Tripwiresecurity.com. An integrity checker applies a mathematical function called "one way" to a file resulting in a "hash." This "one way" function cannot be duplicated, resulting in an original file being created every time. If the file is manipulated in any way without the owner's knowledge, the integrity checker will alert the user that the file has been changed. Like other intrusion detection components, integrity checkers will not prevent crackers from accessing a person's information, they will alert the owner that an event has occurred to a specific file or folder. If a user believes that a file or folder has been modified without his knowledge, he may choose to refer to a backup copy of the same data instead of relying on what could be false information.

Vulnerability Scanners

After the firewall and intrusion detection system have been installed and configured, the next step is to test the home computer's defenses with a vulnerability scanner. Vulnerability scanners are programs that target operator specified IP addresses in an attempt to gather information about the system or systems being scanned. The report generated by a vulnerability scanner can be a valuable tool in narrowing the computer user's focus and thus saving time and energy on attempting to thwart the endless number of threats from the Internet. Once a person has an informed idea of the vulnerabilities on his system, he can focus on correcting the realistic problems, whether it is blocking open ports by fine tuning firewall properties, installing security patches for a specific operating system, or making changes to the intrusion detection system. Some of the information that can be gathered are communication ports being used, the status of the ports such as whether it is open or listening, and the different protocols being used. Some vulnerability scanners such as SARA and Internet Security Services (ISS) Internet Scanner will test for specific vulnerabilities and recommend certain security patches.

Several commercial and freeware versions of vulnerability scanners are available. Internet Security Services Internet Scanner, Norton's NetRecon, and NAI's CyberCop Scanner are the three big names for commercially available scanners. Three very effective freeware vulnerability scanners are Security Auditor's Research Assistant (SARA) which is used on Unix systems and can be downloaded from http://www-arc.com/sara/index.shtml; Nessus can be

downloaded from http://www.nessus.org; and Nmap can be downloaded from http://www.eeye.com (Windows version) and http://www.insecure.org (Unix version).

When new versions of operating systems are created and new options are offered to the consumers, vulnerabilities may be created allowing vulnerabilities for crackers to exploit. If the user is running a Microsoft Windows operating system and is attempting to get a handle on the seemingly endless stream of security patches, he or she has a couple of options. The first option is to take it upon one's self to remember to visit Microsoft's web site periodically and check for patches on the specific operating system and applications being used. The other option, and the one I prefer, is to subscribe to Microsoft's Product Security Notification Service and receive automatic notifications when patches are released. However the owner of the network chooses to approach correcting the vulnerabilities, he should, at a minimum, compare his vulnerability report to the SANS/FBI "Twenty Most Critical Internet Security Vulnerabilities" list which can be viewed and downloaded at http://sans.org/top20.htm. Bob Todd, the creator of SARA, has recently created a version of SARA that will specifically scan for the twenty most critical Internet security vulnerabilities which, like the original version of SARA, is freeware.

To be effective, the vulnerability scanner needs to be run against the home network periodically. New threats emerge daily that are designed to beat current security postures. A user must continue to test his defenses if he is to remain secure. How often the vulnerability scanner is run depends on factors such as if the computer has been compromised, if new threats have been identified, or if a new operating system or other software has been loaded on the computer. Changes to the threat environment and computer system warrant conducting a new scan.

Updated Virus Protection

The last line of defense in protecting the home computer is anti-virus protection. Even with a properly configured firewall and an intrusion detection system running, an infected e-mail or program laced with malicious code may be open or executed, then the firewall and intrusion detection system cannot protect or save the computer. An anti-virus protection program such as Norton or McAfee must be installed. According to the McAfee Anti-Virus Emergency Response Team (AVERT), "over 500 viruses are discovered each month…" (Microsoft, 2000). These new viruses do not discriminate between corporate and home computers. They are looking for vulnerabilities in any system. Because of the number of new viruses discovered, it is just as important that the user update virus definitions on a regular basis to round out overall computer security. Having outdated virus protection on one's computer is like locking the doors to the car and leaving the windows cracked enough for a car thief to stick his arm in.

McAfee.Com has provided, "Virus Detection and Prevention Tips" which lists ten simple tips to help prevent one's system from getting infected. These tips are summarized below:

1. Don't open any files attached to emails from strangers.
2. Don't open files attached to emails unless you know what the file is EVEN IF IT APPEARS TO COME FROM A FRIEND.
3. Don't open files attached to email if the subject line is questionable.
4. Delete chain emails and don't contribute to their spread.
5. Don't download files from strangers.
6. Be cautious when downloading files from the Internet.

7. Update anti-virus software regularly.
8. Back up files regularly.
9. Always err on the side of caution when downloading anything.
10. If in doubt, notify an authority such as McAfee or Norton concerning questions about a possible virus.

If home computer users follow these basic tips, they stand much less of a chance of infecting their systems with a virus.

Frequent Back-Ups

What happens when you have taken every reasonable effort to secure the computers on your home network and disaster strikes: a new virus is introduced to the system or a natural disaster such as a basement floods destroying all of that important data? What now? Well, hopefully, the user has a recent back up of all his data. Backing up data is one of the most important, yet one of the most overlooked steps in the home environment. Periodically backing up the hard drive to a tape drive, CD rewriter, or an external hard drive could save a person a lot of work when needing to rebuild the hard drive or recover damaged files.

Network security is a very fluid environment. New threats emerge daily, new operating systems and applications offer new challenges in securing data, and crackers are constantly developing new ways to exploit computer systems. Home computer systems have been added to the computer security battlefield. The only way to remain as safe as possible on the Internet and protect the availability, integrity, and confidentiality of personal information stored on the computer is to take an active role in home computer security. This can be accomplished by remaining educated regarding your operating system, the different security tools at your disposal such as personal firewalls, intrusion detection systems, vulnerability scanners, anti-virus protection, and by remaining diligent about installing updates on your software, maintaining caution when dealing with suspicious email, and backing up your data on a regular basis. Applying some basic security tools and procedures at home will go a long way to preventing your home computer from being used by a cracker to access your personal, corporate and financial information, or to use your computer to launch attacks against other computers and networks.

References

Boran, Sean. (28 Sep 2001). An Analysis of Mini-firewalls For Windows Users. [On-line]. Available: http://www.boran.com/security/sp/pf/pf_main20001023.html

Cohen, Adam. (30 April 2001). Hands Off My PC! Time Magazine. [On-line database] Wilson Select Plus.

DoSHelp-Intrusion and Attack Report Center. (13 Nov 2001). Trojan and Remote Access Service Ports. [On-line]. Available: http://doshelp.com/trojanports.htm

eTango. (15 Dec 2001). Market Statistics. [On-line]. Available: http://www.etango.com

Internet Assigned Numbers Authority. (11 Dec 2001). Port Numbers. [On-line]. Available: http://www.iana.org/assignments/port-numbers

McAfee Anti-Virus Emergency Response Team. (10 Dec 2001). Virus Detection and Prevention Tips. [On-line]. Available: http://dispatch.mcafee.com/virus_tips.asp?cid=1593

Microsoft TechNet. (Dec 2000). Product Security Notification. [On-line]. Available: http://microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/notify.asp

"North America DSL Market Reaches 600,000 Lines in 1999" (Feb. 17, 2000). Boston, Business Wire. [On-line]. Available: http://www.businesswire.com/webbox/bw.021700/200481325.htm

"North America DSL Market Reaches 4.7 Million" (Nov. 21, 2001). Boston, Business Wire. [On-line]. Available: http://www.xdsl.com/content/tcarticles/wp112701.asp

Russell, D. & Gangemi, G.T. Sr. (1991). Computer Security Basics. O'Reilly & Associates, Inc.

The SANS Institute. (2001). Security Essentials-Network Security. Bethesda, MD.

---. (2001). Security Essentials-Networks, Routers, & Firewalls. Bethesda, MD.

---. (2001). Security Essentials-The Big Picture. Bethesda, MD.

---. (2001). The Twenty Most Critical Internet Security Vulnerabilities – The Experts' Consensus. [On-line]. Available: http://www.sans.org

Trans-Atlantic Communications. (18 Apr 1994). Net BSD Reference Manual. [On-line]. Available: http://www.tac.eu.org/cgi-bin/man-cgi?netstat+1

Questions.

1. Which of the following could be classified as an event?
   A) computer rebooting
   B) file being deleted
   C) application executing
   D) All of the above
   The answer is D. An event is any observable occurrence in a system and/or network.

2. An integrity checker applies a mathematical function to a chosen file or folder called a:
   A) hash
   B) mark
   C) one way
   D) identifier
   The answer is C. An integrity checker applies a mathematical function called "one way" to a file resulting in a "hash."

3. Of the following items listed, which is not part of a Microsoft Netstat report:
   A) Type of communications protocol being used
   B) Local IP address
   C) Remote IP address
   D) Amount of time connected to remote user
   The answer is D. The first column lists the type of communication protocol being used such as Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). The second column lists the local IP address port number. The third column lists any foreign IP address that may be talking to the local address. The fourth column lists the state of the local address such as whether the local address is listening or communicating with a foreign address.

4. According to McAfee's Anti-Virus Emergency Response Team (AVERT), the number of new viruses discovered each month exceeds
   A) 200
   B) 300
   C) 400
   D) 500
   The answer is D. "over 500 viruses are discovered each month…" (Microsoft, 2000)

5. Of the following security layers, which should be employed in the home environment?
   A) a well configured firewall
   B) an intrusion detection system
   C) routinely updated virus protection
   D) periodic back up of the data stored on a home computer
   E) all of the above
   The answer is E.

1. Events are always considered malicious in nature.
   True
   False
   The answer is false. Events are not necessarily bad or malicious in nature; a file being deleted from a computer by a user is a normal event. However, an event is malicious in nature when a virus causes the same file to be deleted without the user's knowledge. At this point, the event becomes an incident.

2. Firewalls can only prevent traffic from *entering* a network or computer.
   True
   False
   The answer is false. Some personal firewalls can block outgoing traffic, also known as egress filtering, as well as incoming traffic, known as ingress filtering, while other personal firewalls only have ingress filtering capability.

3. Egress filtering is the filtering of message traffic attempting to enter a network or computer.
   True
   False
   The answer is false. Some personal firewalls can block outgoing traffic, also known as egress filtering, as well as incoming traffic, known as ingress filtering, while other personal firewalls only have ingress filtering capability.

4. E-mails with unknown attachments that appear to come from trusted friends are completely safe to open.
   True
   False
   The answer is false. Don't open files attached to emails unless you know what the file is EVEN IF IT APPEARS TO COME FROM A FRIEND.

5. An intrusion detection system can prevent malicious code from executing on a computer or network.
   True
   False
   The answer is false. An intrusion detection system will not prevent someone from gaining access to a computer, but it will notify the user of suspicious activity on communications ports.

Last Updated: July 25th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	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
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
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event