Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Defense in Depth and the Home User: Securing the Home PC

The Internet has permeated the modern world. Business entities rely on the Internet for conducting commerce and trade. Home computer users have discovered the benefits of using the Internet for personal business, communication, education and pleasurable pastimes. In addition to the array of benefits the Internet provides, come associated risks. Such risks may include, but are not limited to, viruses, software vulnerabilities, and unsafe computing practices. While businesses are generally well informed and take measures...

Copyright SANS Institute
Author Retains Full Rights

AD
nitrosecurity Log Management

Defense in Depth and the Home User:

Securing the Home PC

GIAC Security Essentials Practical Assignment
Version 1.4b

By

Shauna Munson

January 24, 2003

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Introduction

The Internet has permeated the modern world. Business entities rely on the Internet for conducting commerce and trade. Home computer users have discovered the benefits of using the Internet for personal business, communication, education and pleasurable pastimes. In addition to the array of benefits the Internet provides, come associated risks. Such risks may include, but are not limited to, viruses, software vulnerabilities, and unsafe computing practices. While businesses are generally well informed and take measures to protect against these risks, the home computer user is typically unaware and ill prepared to protect their system from threats associated with Internet usage. Although it is impossible to provide full and complete protection from all threats, applying the principles of defense in depth to the home computer will reduce Internet-based risks, and produce a well-secured home computer. This document is written with the home computer user as the target audience. Its purpose is to make the home computer user aware of the risks of using an unsecured computer, and to provide a guide in how to secure the home computer by applying various layers of defense to their system. Part 1 will discuss the need for defense in depth at home. Part 2 will serve as a guide to securing the home computer and following safe computing practices.

Part 1: The Need for Defense in Depth at Home

The Risks

The Internet has become an integral part of everyday life for many people: email, web surfing, chat, and file sharing have literally become a part of life, and an indispensable form of communication. The Internet has the potential to enrich our lives from the benefits that it has to offer—a vast wealth of information at our fingertips that we can tap into at any given moment, as well as the convenience of online services such as banking, shopping, and investing. There are more homes connected to the Internet than ever before with ever-increasing numbers utilizing high-speed connections through means of Cable or DSL (digital subscriber lines). Just as any medium that is used as a tool for good, there are those who use it just as effectively as a tool for mischief, and malicious deeds.

The home computer has become a ripe target for those with mal intent. Many home users overlook, or are unaware of the need to secure their computer. Many are unprepared to tackle the risks associated with using the Internet. The need to educate the home user to the risks of using the Internet and to provide information on how to secure their computer against these risks has never been greater.

Remember the phrase 'Ignorance is bliss?' Well, not where the Internet is concerned! Many users believe that their home computer does not contain anything of interest to others and may wonder why security is important for their home computer. Consider for a moment what you do with your home computer

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

and what is stored on it: online banking and shopping; email; financial statements; tax records; credit card numbers and investment account information; as well as other personal information that may be stored. Would you be comfortable allowing a perfect stranger to view and access this data on your home computer? Probably not.

There are many who want to gain unauthorized access to your computer—they are referred to as intruders, hackers, and attackers. There are many reasons that intruders want access to your computer. These individuals are not interested solely in your data; they may want your computer for its disk space so that they can store stolen or pirated software; they may want your computer for its Internet connection; they may want to remotely control your computer; they may want to use your computer to help them launch an attack against someone else.[1] An intruder will do this without the knowledge of the computer owner.

The next question is how do intruders get access to your computer? Intruders often gain access through vulnerabilities (frequently called holes) which exist in computer software. When a hole is found, software vendors will usually provide a patch to fix the problem (closing the hole). Default settings in programs often make a computer more vulnerable to unauthorized access. Trojan horse backdoor programs are popular ways that intruders gain access to your computer. These programs will disguise themselves as a game or some other type of harmless software. When the user installs the program, unbeknownst to him, he is also providing the means for an intruder to access the PC at will and do whatever he desires with the computer. Social engineering is another very popular and effective technique used by intruders. Social engineering is the art of using persuasion or deception by manipulating human vulnerabilities. For example, while you are online, a popup message appears from your 'Internet Service Provider', stating that they are updating their records and need to confirm your password and credit-card information. Sounds like a legitimate request, so you reply with the information requested, without considering that you are actually sending this sensitive data to a computer hacker (a reputable Internet Service Provider would not request this information via a pop-up dialogue box).

There exists the risk of home computers being used as 'zombies' in a Distributed Denial of Service (DDoS) attack. This is when your computer is used to attack another computer somewhere on the Internet. 'Zombie' is a term that refers to a computer that has been compromised with a program that runs a process or service in the background—once again unknown to the user—that listens for instructions through an open port from the hacker that put it there. (A port is a means of allowing access to a computer. A port can be open or closed, similar to doors and windows on a house. If a door or window is securely closed, outsiders cannot come in; if it is left open, anyone from the outside can enter.) A hacker may have literally hundreds or thousands of compromised computers at his command. At a designated time, he will issue a command to his army of zombies (remember, they are listening for instructions from their 'master'—the hacker's computer—through an open port) directing them to start sending thousands of packets or pieces of information to the same target, usually a web site (yahoo.com, for example), all at the same time. The server on the targeted

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

web site becomes overloaded with useless packets, and is unable to respond to valid requests thereby denying service or access to legitimate users of the web site. Guess what! Your computer has just become an accomplice in a DDoS attack. A compromise of this type is a serious threat to the Internet as a whole, taking down web sites for many hours at a time (some well-known sites that have been victims of this are yahoo.com, amazon.com and cnn.com[2]).

Another concern for home computer security is the fact that increasing numbers of people are telecommuting and taking work home, in addition to maintaining files on both their home computer and their work computer. An attacker could have a very difficult time trying to gain access to a well-secured corporate network, but could find it quite easy to access sensitive files on an employee's unsecured home computer. The threat of corporate espionage is very real, and should be of concern to any business that allows its users remote access to the corporate network from home. Lax security of a home PC poses a security risk to the corporate network when the user is connected from home.[3]

Hackers have determined that home computers are vulnerable to compromise. They are easy targets, and attacks against these systems are very successful. Research by the CERT Coordination Center concluded that hacker attacks against home computers are on the rise, and in many instances, "hackers are using home PC's to gain access to corporate networks."[4]

The Solution: A Layered Approach to Securing the Home PC

All of the previously mentioned risks can adversely affect three main areas: the confidentiality of your information (i.e. intruders may be able to view your files); the integrity of that information (i.e. intruders can change or alter your files); and availability (the ability to access your information when you need it). Security professionals responsible for protecting corporate networks from attack know that the best approach to protecting the confidentiality, integrity and availability of the network, is a layered approach. This same approach can be applied very effectively to the home computer. Layers of defense will make a home computer much more difficult to compromise. This will provide immediate benefits to the home user in the form of a safer, more secure, and enjoyable Internet experience. Vitally important is the fact that the home computer will no longer be an easy target. This is an essential step toward securing the Internet as a whole.

There are a number of actions the home user can take to secure their home computer and apply principles of defense in depth. The remainder of this document will serve as a guide to educate the user in how to make the home computer more secure. Each section of the guide is a layer of defense. One layer by itself does not make a computer secure, however the layers combined, will make for a well-protected home computer.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Part 2: Guide to Home PC Security

Remember when I mentioned the phrase 'Ignorance is bliss?' Well, now we are going to turn that around, and coin the term 'Knowledge is power.' Much of the lax security of home computers can be attributed to a general lack of knowledge and awareness pertaining to the risks of using an unsecured computer. When a home user becomes aware of the risks and knows how to protect themselves against said risks, that is where the power comes in. The home PC user now has the power to protect themselves from Internet threats.

Virus Protection with Automatic Updates Enabled

The first layer of defense to apply to the home PC is adequate and up-to-date antivirus software. Prior to the explosive growth of networking, the most common way to obtain a virus was from an infected floppy disk used at home or at school, and then used someplace else, such as the workplace. However, with the growth and popularity of the Internet and email, there are new and more efficient means of delivering a virus. The result is that viruses now multiply and spread faster than ever before. Viruses are a significant threat, and an unprotected system is sure to be infected with a virus sooner, rather than later.

So what exactly is a virus? A virus is a manmade program that is run on a computer without the knowledge or permission of the user.[5] Trojan horses and worms are other terms you may have heard that are often lumped together with viruses. A worm is like a virus on autopilot: it does not require user intervention and spreads by replicating itself to other computers connected to a network or the Internet. Viruses can spread via floppy disks; CD-ROMs; email; web sites; and file downloads. Viruses are dangerous as they frequently cause damage by carrying out malicious deeds, such as deleting files, formatting your hard drive or installing backdoor programs (referred to as trojans) such as NetBus or BackOrifice. Installation of backdoor Trojans create a point of entry to your PC, much like leaving the back door to your home open for anyone to enter. This allows a hacker to return to your computer, gain entry, and take control of your PC.[6]

There are various types of viruses: program, boot record, and macro viruses for example. They can target program files (such as files with .exe or .com extensions), boot records on disks (i.e. floppy disk and hard drives), and likewise can target data files (such as Word or Excel files). Some viruses require the user to run a program (such as Word) in order to unleash the virus; others can spread to the boot record of a disk, loading at startup. Additional means of obtaining a virus are by downloading an infected file from the Internet (file sharing programs are such as Kazaa and Morpheus are common ways to get a virus); going to a web page that tries to push out a virus to the user simply by visiting the web site; yet others are spread as attachments to email. Two very well known examples are the ILOVEYOU virus and the Melissa macro virus. When the email attachment was opened, the virus used the Outlook address book to email itself to other users, and so on.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Viruses have also become more intelligent in recent years. Some viruses use email spoofing, i.e. making it appear that the virus came from you, when it really didn't—the virus simply grabbed your name and email address from someone who had you in their address book, and put it in the senders name to hide where the email actually originated from. Depending on the code of the virus, they can attempt to avoid detection through various stealth methods. A stealth virus changes itself to avoid detection, and may disable the antivirus software used to detect them.

Antivirus software can protect your system from viruses (including worms, trojan horses and other malicious software). However, in order for antivirus software to be effective, it is critical that the virus signatures be up to date. When a new virus, worm, or other type of malicious software hits, the software vendor will update their signature file to detect the new virus. These signature files are typically updated every few days and can be downloaded from the vendor's website. This is where many users fall short—they fail to update their virus software regularly—rendering their home computers vulnerable, and in many cases actually contributing to the spread of viruses, instead of protecting against them.[7] At a minimum, users should check the software vendor's website for signature updates at least once a week.

In order to be effective, antivirus software should provide real time protection capabilities. It should allow automatic updates of signature files (thus solving the problem of users failing to manually update signature files), scan all email and attachments, downloaded files, compressed files and provide the ability to scan any file before opening it. It is also advised to schedule a regular virus scan of your hard drive, either weekly or bi-monthly.

Attackers have had a lot of success with viruses and other malicious software, and continue to do so. Using an antivirus program and keeping it current is critical to securing your home computer.[8] This layer of defense cannot be neglected!

Exercise Caution Opening Email and Email Attachments

Email has become an effective means of spreading viruses and worms. If you have not been the victim of an email-born virus or worm, you probably know somebody who has. It used to be that you could not get an email virus unless you opened the attachment. That is no longer the case! With HTML email (email that looks like a web-page when opened), a virus or worm may be spread by merely opening the email; even if the email does not contain an attachment. Furthermore, if you have the 'preview pane' feature enabled in your email software (see Figure 1), you do not even have to open the email. The preview pane feature allows you to see the contents of an email by highlighting the email in your inbox. Simply highlighting the message can trigger and spread the virus;[9] so it's a good idea not to use the preview pane feature in your email program.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

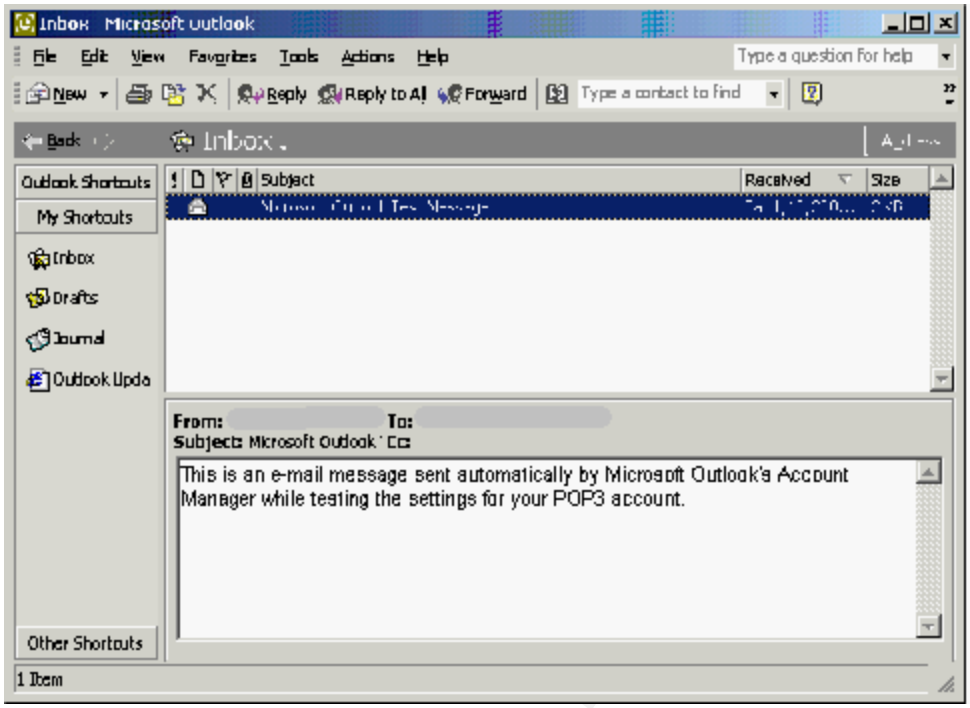

Figure 1

One way that email viruses victimize many people is by falling prey to some type of social engineering trap. As previously mentioned, social engineering aims to manipulate or deceive someone by exploiting human vulnerabilities. Email with attachments in the form of social engineering often fools the unsuspecting or curious recipient into opening the attachment. Even virus-conscious users can fall prey to social engineering. A great example of this is an email going around that claims to be a "free immunity tool that will protect your PC from the Klez.E virus." Here are the contents of the message:

> Subject: Worm Klez.E Immunity
>
> Klez.E is the most common world-wide spreading worm. It's very dangerous by corrupting your files. Because of its very smart stealth and anti-anti-virus technic,most common AV software can't detect or clean it. We developed this free immunity tool to defeat the malicious virus. You only need to run this tool once,and then Klez will never come into your PC. NOTE: Because this tool acts as a fake Klez to fool the real worm,some AV monitor maybe cry when you run it. If so,Ignore the warning,and select 'continue'. If you have any question,please mail to me.[10]

Some of the information in the message is correct, but it does not contain an 'immunity tool'. In fact, by opening the attachment, the virus itself is actually unleashed! Pretty clever! In this example, use common sense—if it tells you your virus software will not like it and will warn against it, that in itself sounds suspicious! Go to a reliable, trustworthy source, such as Symantec.com or your antivirus vendor's website to get more information.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

A secondary example is the ILOVEYOU virus. Who could resist opening an attachment called "loveletterforyou.txt?" Well, many could not! It appeared to be a harmless text document, right? What most home users didn't see is that this attachment actually had a double file extension—the file was actually called love-letter-for-you.txt.vbs (a .vbs file is a visual basic script or program, that is run when the attachment is opened, similar to an .exe file.) So, if the user had Windows set to 'hide file extensions' they would not have known that it was not a harmless text file, but a potentially dangerous 'executable' file. This is a simple Windows setting that all users should disable (see section entitled Registry Tweaks and Windows Settings for instructions). Disabling this setting will prevent the user from being fooled by double file extensions.

Prior to opening any email attachments, be sure that you know the sender: never open an attachment from a source that you don't know. Are you expecting an attachment from someone that you do know? Even if you know the sender, that is not a good enough reason to justify opening the attachment—especially if you're not expecting it. Many viruses send themselves to the addresses contained in an address book. Even though you may know the sender, he or she may not have legitimately sent the message. If you need to open an attachment, be sure that your virus definitions are current, save the file to your hard drive, and scan it with your antivirus software. Once the file has been scanned then open the file.[11]

The Federal Computer Incident Response Center (FedCirc) suggests a series of five tests[12] that an email must pass before being opened:

1. Know Test: Do you know the sender—if not, that's a red flag.
2. Received Test: Have you ever received email from the sender before or is this the first time—another red flag.
3. Expect Test: Were you expecting an email attachment from the sender? If not—red flag.
4. Sense Test: Does it make sense to be receiving an email from this particular sender, with the contents such as they are described in the "subject" line and attachment name? Does that seem normal—does it make sense? For example, does it make sense to be receiving an attachment called sexxymovie.mpeg from your mother?
5. Virus Test: Does the email contain a virus? This test requires you to have installed and be using an antivirus program (which you should be doing anyway).

If any test fails, that is an immediate red flag: the message should be deleted. Even if the message passes all the tests, you should still be cautious when opening attachments, and monitor for strange or unexpected behavior.

A Well-Patched Operating System

The third layer of defense to apply to a home PC is a well-patched operating system. Many home users may not be aware of the need to apply

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

patches and service packs to their system. For example, when a new operating system is installed, right from the start, it will be lacking in various patches and service packs which fix holes or vulnerable areas in the system (a patch or hotfix addresses a single problem or issue; a service pack addresses multiple issues and may also enhance the operating system). Microsoft is constantly putting out new patches to fix these holes. These holes and vulnerabilities are typically well-known to the hacker community. Hackers have a variety of scanning tools at their disposal to search for specific types of vulnerabilities. Once a vulnerability is discovered, the hacker can later attempt to exploit it. From the authors of Hacking Exposed Windows 2000:

> Applying the most recent service packs and hotfixes from Microsoft for the operating system and all applications (IE, SQL Server, and so on) is perhaps one of the most important steps you can take to secure Windows…. The greatest security risk comes from vulnerabilities that are widely published and generally addressed by a security bulletin and / or patch from Microsoft. Since such vulnerabilities are so widely known, and the Internet community typically distributes exploit code for such issues with prompt regularity, they represent the highest risk to your Windows… [System]. It is thus imperative that you apply the patches for these vulnerabilities (Scambray and McClure, p. 454).[13]

Therefore, a vital layer of defense in depth is to make certain that your home computer is up-to-date on service packs and hotfixes. It is the user's responsibility to install these patches. This will be an ongoing and continual process: doing it just once will not be sufficient. An easy and somewhat painless way to accomplish this is to use Windows Update (go to your 'Start' button, and select 'Windows Update'). This will take you to the Microsoft Windows Update site. The first time you visit the site, you will be prompted to install any required Windows Update software. Next click 'Scan for Updates.' The site will scan for updates (hotfixes, service packs, and drivers) to your computer, after which it will provide a list of critical and suggested updates for your system. It will allow you to select which updates to install, then it will install them to your PC. (Note: when installing patches it is important to install the patch according to the release date, as newer patches are often dependent on updated files from prior patches.) Windows XP can check for updates automatically and notify you when updates are available for your computer. To access this setting, right-click on My Computer and select the 'Automatic Updates' tab.

Use a Firewall

A firewall improves the security of computers that are connected to the Internet or a network by keeping intruders out and letting authorized visitors (data/information) in. A good analogy of what a firewall does will make it easier to understand.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Suppose you plan a trip to another country. Upon your arrival, you must go through a designated point of entry, such as customs or a border checkpoint. At the checkpoint, officials stop you and inspect your documents (such as a passport) to see if you meet the necessary criteria. If everything is in order, you are permitted entry and can continue on to your final destination within the country. If you do not have proper documentation, or if something is not right, the officials will not allow you to pass—your access will be blocked.

This is, in essence, the purpose of a firewall. It will stop and inspect all data or information that arrives at the entry point of your system (known as ports). It will determine if the data should be allowed to pass or if it should be blocked. Firewalls do the same for data that is leaving your computer. Firewalls govern access based on rule sets.[14] Firewalls can be software-based, or hardware-based.

A software-based firewall (sometimes referred to as a personal firewall) is a specialized software program designed to run on individual computers. This type of firewall uses popup windows to notify you of incoming or outgoing access attempts (see Figure 2):

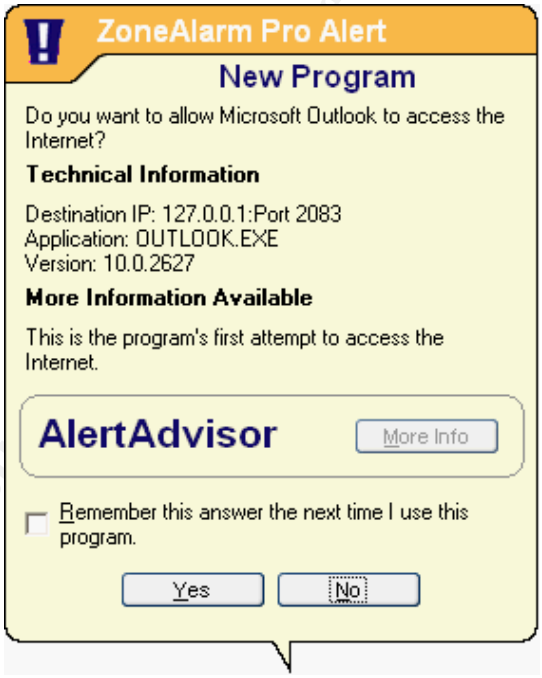

Figure 2

Software firewalls are a good choice for home users with dial-up connections and for those that frequently travel with a laptop computer. Some examples of software-based firewalls are Zonealarm; Sygate Personal Firewall; and Norton Personal Firewall. Zonealarm has a free version available that can be downloaded from www.zonelabs.com.

A hardware-based firewall is a dedicated external device designed to protect a private network from unauthorized access. A hardware firewall should be considered *required* equipment if you have a high-speed Internet connection. There are many good and affordable hardware-based firewall products available

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

made specifically for high-speed Cable and DSL connections (D-Link, Linksys and NetGear are a few). These devices will effectively mask your home computer's IP address making it invisible to outside intruders. It does this through a process called Network Address Translation (NAT).[13]

Spyware Protection

Did you know that someone could be tracking you as you use the Internet? Spyware or adware is software that secretly monitors and collects information on a user's Internet activity and reports that information back to a third party. Spyware is typically downloaded from the Internet as part of shareware or freeware: for example, by downloading peer-to-peer file sharing software. Spyware poses a number of problems. Among these are matters of ethics and privacy. It is installed and runs without the user's knowledge when they install something else. It is typically used for advertising purposes, however it can also collect data about email addresses, monitor keystrokes, collect passwords, scan files, read cookies, install other spyware software, and even change the browser's default home page. All this information is sent back to the spyware author who may use it for advertising and marketing, or they may compile the information to sell to other parties. In addition, Spyware utilizes memory and system resources on your computer, as well as valuable bandwidth on your Internet connection when it phones home.

Two programs created to detect and remove spyware are Ad-aware by Lavasoft (http://www.lavasoftusa.com/) and SpyBot Search & Destroy (http://security.kolla.de/). Both can be downloaded for free from the corresponding web sites. These products scan the memory, registry, and hard drives for spyware and other suspicious items, and allow you to remove them without harming your system (see Figure 3). They also update their signature files (similar to antivirus software) to catch new strains of spyware. If you suspect that a piece software you want to download may contain spyware, www.spychecker.com may be of some assistance. This website contains a database of known spyware. Another very informative site on spyware is www.spywareinfo.com.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

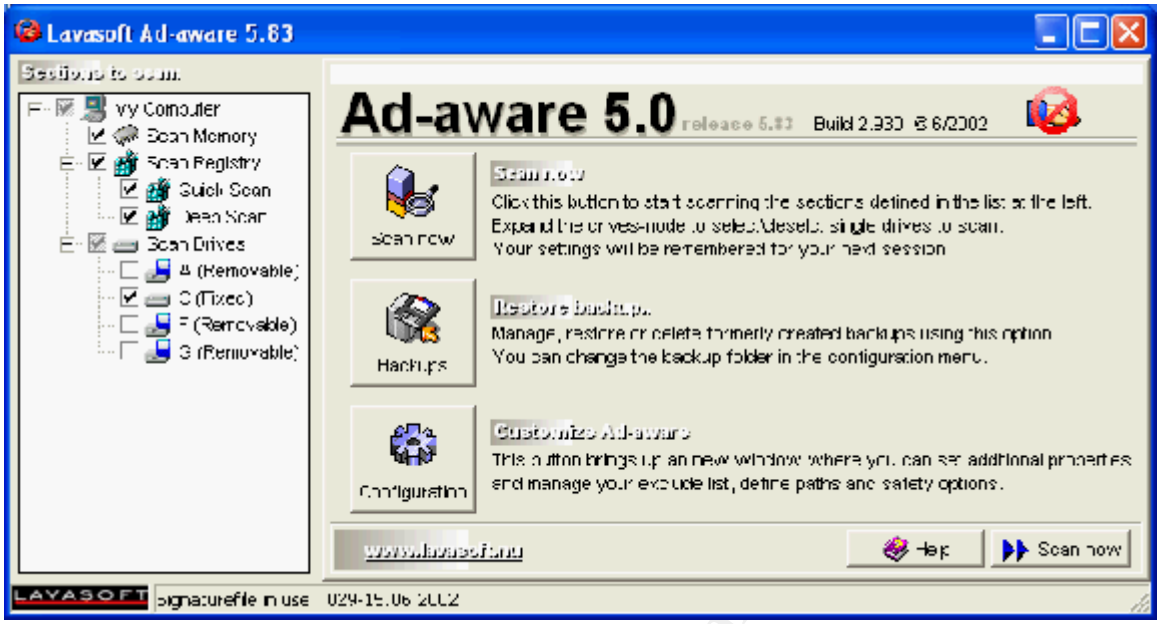

Figure 3

Registry Tweaks and Windows Settings

There are some settings in Windows, often enabled by default, that make a computer less secure. Home users are often unaware of the potential consequences of these default settings, while attackers are well versed in the subject and use default settings to their advantage. With a few registry tweaks and some adjustments to your Windows settings, you can add yet more protective layers to your system. (Note: Making changes to the registry can cause serious problems and could necessitate reinstalling the operating system. If you have never made any changes to the registry, please reference: Editing the Registry. URL: http://www.winguides.com/registry/article.php?id=1&page=3 and the Microsoft Knowledge Base article: Description of the Microsoft Registry. URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;256986. These articles provide instructions on how to backup, edit and restore the registry for Windows, however, if you are uncomfortable editing the registry, it is best left alone.)

Registry Tweaks:

- Disable Anonymous Enumeration (Windows 2000/XP)

Windows supports a special account called the Null or Anonymous user. This account has no username or password, yet is permitted to access certain information from a PC attached to the network (Internet). The Null user can enumerate (detail) account names and open shares on any PC connected to the

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

network. To prevent anonymous enumeration (this is not available for Windows 98/ME users) edit the registry as follows (see Figure 4):

1. Open the registry and find the following registry key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA
2. Change the existing value of "RestrictAnonymous", or create a new DWORD value if it doesn't already exist.
3. Set the Value Data to equal '2'.
4. Restart your computer for the changes to take effect.

Note: *Users must be using a minimum of Windows NT 4.0 with Service Pack 3 for this setting to be enabled.*

(Default)	REG_SZ	(value not set)
RestrictAnonymous	REG_DWORD	0x00000001 (1)

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA

Registry Settings
System Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA] **Value Name:** RestrictAnonymous **Data Type:** REG_DWORD (DWORD Value) **Value Data:** (0 = allowed, 1 = restricted, 2 = require anonymous permissions)

Disclaimer: Modifying the registry can cause serious problems that may require you to reinstall your operating system. We cannot guarantee that problems resulting from modifications to the registry can be solved. Use the information provided at your own risk

Figure 4[15]

- Disable Default Shares

When networking features are enabled on a Windows machine, certain system folders are shared for administrative purposes. A share enables other users to access drives and folders on a computer. The default shares created by

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Windows are: C$ (the C drive) and Admin$ (the Windows System folder), both of which are vulnerable to anonymous enumeration. To disable default shares, edit the registry as follows (See Figure 5):

1. Open the registry and find the following registry key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters
2. Change the value of AutoShareServer and AutoShareWks, or create a new DWORD value if they do not exist.
3. Set the Value Data to equal '0' to disable default shares.

Note: *The shares are normally accessed via \\server\c$ and \\server\d$ depending on the drive letter.*

(Default)	REG_SZ	(value not set)
AutoShareWks	REG_DWORD	0x00000000 (0)
AutoShareServer	REG_DWORD	0x00000000 (0)

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanS...

Registry Settings
System Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters]
Value Name: AutoShareServer, AutoShareWks
Data Type: REG_DWORD (DWORD Value)
Value Data: (0 = disable shares, 1 = enable)

Disclaimer: Modifying the registry can cause serious problems that may require you to reinstall your operating system. We cannot guarantee that problems resulting from modifications to the registry can be solved. Use the information provided at your own risk

Figure 5[16]

Windows Settings:

- Disable Auto-Run

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Auto-run allows CDs to be played automatically when a CD is inserted into the drive. The danger associated with this setting is that the CD could contain a virus or some other form of malicious code, which could be launched when the CD is inserted into the computer. To prevent CDs from playing automatically, auto-run needs to be disabled.

For Windows 98/ME:

To disable the feature that allows CD-ROMS and audio CDs to run automatically:

1. Click **Start**, select **Settings**, click **Control Panel**, then double-click **System**.
2. Double-click the **CDROM** branch on the **Device Manager** tab, and then double-click the entry for your CD-ROM drive.
3. On the **Settings** tab, click to clear the **Auto Insert Notification** check box.
4. Click **OK**, click **Close**, and then click **Yes** when you are prompted to restart your computer.[17]

For Windows 2000/XP (see Figure 6):

1. Open the registry and find the following registry key:
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CDRom
2. Change the value of 'Autorun', or create a new DWORD value if it doesn't already exist.
3. Set the Value Data to equal '0' to disable the Auto-run feature.
4. Restart your computer for the changes to take effect.

Note: *This method disables automatically running CD-ROMs. If you want to disable automatically running CD-ROMs depending on the CD-ROM that you insert in the CD-ROM drive, you can press and hold down one of the SHIFT key while you insert the CD-ROM.*

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

(Default)	REG_SZ	(value not set)
Autorun	REG_DWORD	0x00000000 (0)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CDRom	

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Registry Settings
System Key: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CDRom] **Value Name:** Autorun **Data Type:** REG_DWORD (DWORD Value) **Value Data:** (0=disable, 1=enable)

Disclaimer: Modifying the registry can cause serious problems that may require you to reinstall your operating system. We cannot guarantee that problems resulting from modifications to the registry can be solved. Use the information provided at your own risk. (http://www.winguides.com/registry/display.php/6/)

Figure 6[18]

- Disable Hidden File Extensions

A default installation of Windows will automatically hide the three-letter file extension. For example, when viewing files in Windows Explorer or My Computer, the user will see only a file called 'setup' instead of a file called 'setup.exe.' This can be risky, especially where email attachments are concerned. As previously discussed, a user can be fooled by double file extensions, or execute a file simply because they did not know it was an executable due to the hidden extension. This is a simple Windows setting that all users should disable by unchecking the box in the Folder Options window. Here's how:

1. In **My Computer** or **Windows Explorer**, go to the **Tools** menu (in Windows 98, go to the **View** menu).
2. Select **Folder Options**.
3. Click on the **View** tab.
4. *Uncheck* "**Hide extensions for known file types**" (see Figure 7).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

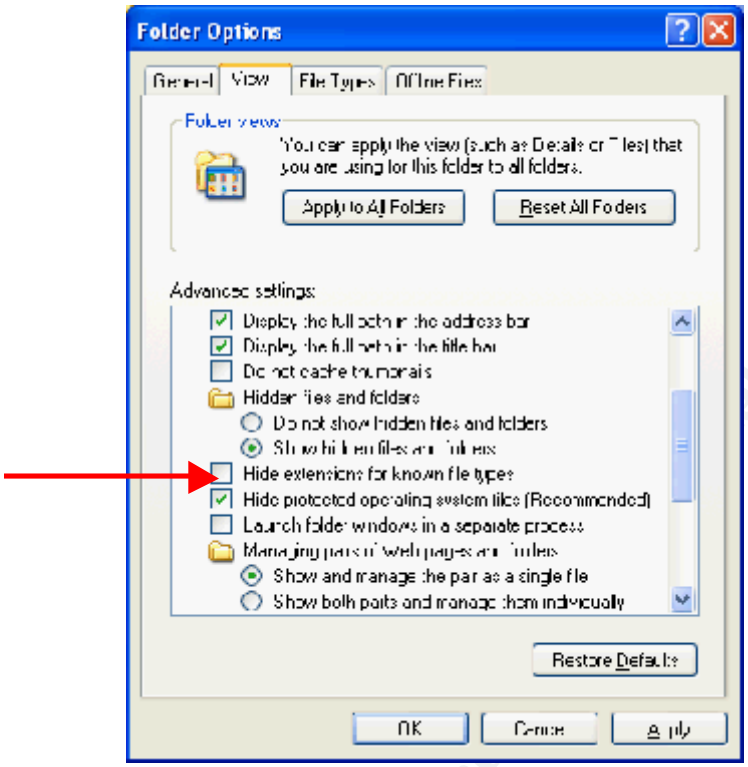

Figure 7

- Disable File and Print Sharing

Microsoft Windows allows files to be shared via the Internet. This is true regardless of whether you have a dial-up modem or high speed connection. This capability can allow intruders to potentially infect your computer with a virus and/or look at files on your computer. If you have enabled this feature, this was probably not your intention. Unless you have a specific need for File and Print sharing, for security purposes, it is prudent to disable this feature.

<u>Windows 98/ME:</u>

1. Click **Start**, select **Settings**, Click **Control Panel**, then double-click **Network**.
2. Select the **Configuration** tab
3. Click the **File and Print Sharing** button.
4. **Uncheck** each box, and click OK.
5. Click **OK** again. If prompted to restart your computer, click **yes**.

<u>Windows 2000/XP</u>

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

1. Click **Start**, select **Settings**, Click **Control Panel**, then double-click **Network and Dial-Up Connections** (in 2000) or **Network Connections** (Windows XP).
2. Right-click on **Local Area Connection** and select **properties**.
3. Select the **General** tab
4. Uncheck the box entitled "**File and Printer Sharing for Microsoft Networks**."
5. Click **OK**.
6. Click **OK** again. If prompted to restart your computer, click **yes**.

Backup Important Data

What do you store on your computer? Financial records, digital photos, important files, special projects, or perhaps you work from home and store all your work on the computer? What if something happened to your computer? Theft, fire, earthquake, hard drive crash, you accidentally delete an important file, or a virus or hacker destroys or alters your files? If something were to happen to the data, would it be lost forever? In order to preclude any of the aforementioned scenarios, you need to make backups. There are commercial software products available (see www.ntibackupnow.com and www.stompinc.com) to home computer users to help facilitate the process of backing up, although they are not required in order to perform a backup. Windows 98 through Windows XP have built-in backup applications, but may not have all of the bells and whistles of a commercial product. There are four areas of consideration when planning your backups.

First, you need to decide which files to backup. You probably do not need to backup every file on your computer—that would be somewhat unrealistic as well as time consuming. You can however, back up any specific files or folders that you wish. These should be files that would be hard to recover if they were lost, or that cannot be re-installed from a CD or a floppy disk, such as financial records and photos. A good rule of thumb is to backup files which you cannot replace or recreate.

Second, how often do you need to backup? Ideally, you should backup a file every time it changes. That may not be practical for many people; once a week would be more realistic. Keep in mind that any changes made since the last backup will not be included if you need to recover any of those files. Plan a backup schedule (once a week or once a month) and stick to it—you'll be glad you did.

Third, what type of media can you put your backups on? You can backup data to an external or removable hard drive, a personal tape drive, Zip or Jazz drive, CD-burner or a DVD-burner. Consider which of these you already have available and use it. There are even some online services which allow you to backup your data by sending it to their servers, thus it is stored offsite, yet with the capability of retrieving that data from anyplace you may be with an Internet connection. There are ample alternatives out there for storing your files.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Fourth, how and where should you store your disks after you backup data to them? Well, you need to store them in a safe place—remember that they contain files that are virtually irreplaceable if lost or damaged. Consider a safe, or even a fireproof safe. You may want to store them in another location, such as at the office or in a safety-deposit box.[19] If you do not have a secure storage area, do not let this prevent you from doing regular backups: any backup is better that no backup!

Summary

The Internet has provided the home PC user with an abundance of information; literally at their fingertips. The Internet provides entertainment, financial services, instantaneous worldwide communication, as well as an instrument to provide an enhanced forum for educational purposes. However, there are inherent risks associated with using an unsecured computer on the Internet. As the typical home computer user is neither aware, nor knowledgeable of the threats associated with using the Internet, the home computer is typically unsecured. Hackers have discovered that home computers are an easy target for their antics. Use of an unsecured home computer online, leaves the unsuspecting user vulnerable to a host of Internet-based risks. In many cases, the question is not if the computer will be compromised—it's a matter of when. Providing the home user with awareness of the inherent risks, in addition to equipping them with the tools to mitigate those risks, is a fundamental step in securing the Internet

Defense in depth can successfully be applied to the home computer. The various layers of protection are:

- Virus protection with automatic updates enabled
- Exercise caution opening email and email attachments
- A well-patched operating system
- Use a firewall
- Spyware protection
- Registry tweaks and Windows settings
- Backup important data

Applying the principles of defense in depth provides an effective safeguard against malicious software, Internet intruders, and promotes a safe and enjoyable Internet experience.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

List of References

"7 Steps to Helping Personal Computing Security." 2 Apr. 2002. URL: http://www.microsoft.com/security/articles/steps_default.asp (2 Dec. 2002).

Armistead, Cynthia L. "Yes, You Can Get a Virus By Simply Reading Email Without Opening Any Attachments." 10 May 2001. URL: http://www.technomom.com/writing/emailvirus.html (4 Jan. 2003).

"Automatic Hidden Shares." 3 Apr. 2002. URL: http://www.winguides.com/registry/display.php/4/ (21 Jan. 2003).

Cert Coordination Center. "Home Network Security." 5 Dec. 2001. URL: http://www.cert.org/tech_tips/home_networks.html (3 Dec. 2002).

Computer Associates International, Inc. "Virus Information & Prevention." URL: http://www3.ca.com/Solutions/CollateralList.asp?CCT=19517= (6 Jan. 2003).

"Control the CD-ROM Autorun Function." 17 June 2002. URL: http://www.winguides.com/registry/display.php/6/ (8 Jan. 2003).

Detert, Ryan. "A Basic Guide to Home Network Security." 14 Jan. 2000. URL: http://www.webreview.com/2000/01_14/developers/01_14_00_1.shtml (4 Dec. 2002).

Fisher, Dennis. "Internet Survives Massive DDoS Attack." 23 Oct. 2002. URL: http://www.eweek.com/article2/0,3959,645884,00.asp (5 Dec. 2002).

Granneman, Scott. "Securing Privacy, Part Two: Software Issues." 14 May 2002. URL: http://online.securityfocus.com/infocus/1579 (6 Dec. 2002).

Granneman, Scott. "Securing Privacy, Part Three: E-mail Issues." 25 Apr. 2002. URL: http://online.securityfocus.com/infocus/1573 (4 Dec. 2002).

Hazari, Sunil. "Firewalls For Beginners." 6 Nov. 2000. URL: http://online.securityfocus.com/infocus/1182 (4 Dec. 2002).

McClure, Stuart, Joel Scambray, and George Kurtz. Hacking Exposed: Network Security Secrets and Solutions. 3rd ed. New York: Osborne/McGraw-Hill, 2001.

Microsoft Knowledge Base Article – 126025. "How to Disable the Feature That Allows CD-ROMs and Audio CDs to Run Automatically." 13 Aug. 2001. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;126025 (8 Jan. 2003).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Mikkelson, David P. and Barbara. "Worm Klez.E Immunity" 1 May 2002. URL: http://www.snopes.com/computer/virus/immunity.htm (4 Jan. 2003).

"Restrict Anonymous User Access." 11 Jun. 2002. URL: http://www.winguides.com/registry/display.php/97/ (21 Jan. 2003).

Rogers, Lawrence R. "Home Computer Security" 2002. URL: http://www.fedcirc.gov/homeusers/HomeComputerSecurity/ (28 Dec. 2002).

Scambray, Joel and McClure, Stuart. Hacking Exposed Windows 2000: Network Security Secrets and Solutions. New York: Osborne/McGraw-Hill, 2001.

Steinke, Steve. "Tools for Securing Home Networks." 4 Mar. 2002. URL: http://www.networkmagazine.com/article/NMG20020304S0014 (4 Dec. 2002).

Teel, James. "Securing the Last Unprotected Area of the Network." Nov. 2002. URL: http://www.scmagazine.com/scmagazine/sc-online/2002/article/52/article.html (6 Dec. 2002).

Webopedia. "Virus." 12 Sept. 2002. URL: http://www.webopedia.com/TERM/V/virus.html (30 Dec. 2002).

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

End Notes

[1] Cert Coordination Center. "Home Network Security." 5 Dec. 2001. URL: http://www.cert.org/tech_tips/home_networks.html#I-C (3 Dec. 2002).

[2] Fisher, Dennis. "Internet Survives Massive DDoS Attack." 23 Oct. 2002. URL: http://www.eweek.com/article2/0,3959,645884,00.asp (5 Dec. 2002).

[3] Detert, Ryan. "A Basic Guide to Home Network Security." 14 Jan. 2000. URL: http://www.webreview.com/2000/01_14/developers/01_14_00_1.shtml (4 Dec. 2002).

[4] Teel, James. "Securing the Last Unprotected Area of the Network." Nov. 2002. URL: http://www.scmagazine.com/scmagazine/sc-online/2002/article/52/article.html (6 Dec. 2002).

[5] Webopedia. "Virus." 12 Sept. 2002. URL: http://www.webopedia.com/TERM/V/virus.html (30 Dec. 2002).

[6] Computer Associates International, Inc. "Computer Viruses – An Introduction." 18 Oct. 2001. URL: http://www3.ca.com/solutions/collateral.asp?CID=33330&ID= (6 Jan. 2003).

[7] Computer Associates International, Inc. "Choosing Antivirus Software." 17 Oct. 2001. URL: http://www3.ca.com/solutions/collateral.asp?CID=33335&ID= (6 Jan. 2003).

[8] Rogers, Lawrence R. "Home Computer Security" 2002. URL: http://www.fedcirc.gov/homeusers/HomeComputerSecurity/#1 (28 Dec. 2002).

[9] Armistead, Cynthia L. "Yes, You Can Get a Virus By Simply Reading Email Without Opening Any Attachments." 10 May 2001. URL: http://www.technomom.com/writing/emailvirus.html (4 Jan. 2003).

[10] Mikkelson, David P. and Barbara. "Worm Klez.E Immunity" 1 May 2002. URL: http://www.snopes.com/computer/virus/immunity.htm (4 Jan. 2003).

[11] Cert Coordination Center. "Home Network Security." 5 Dec. 2001. URL: http://www.cert.org/tech_tips/home_networks.html#IV-A-4 (3 Dec 2002).

[12] Rogers, Lawrence R. "Home Computer Security" 2002. URL: http://www.fedcirc.gov/homeusers/HomeComputerSecurity/#3 (4 Jan. 2003).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

[13] Scambray, Joel and McClure, Stuart. Hacking Exposed Windows 2000: Network Security Secrets and Solutions. New York: Osborne/McGraw-Hill, 2001. 454.

[14] Hazari, Sunil. "Firewalls For Beginners." 6 Nov. 2000. URL: http://online.securityfocus.com/infocus/1182 (4 Dec. 2002).

[15] "Restrict Anonymous User Access." 11 Jun. 2002. URL: http://www.winguides.com/registry/display.php/97/ (21 Jan. 2003).

[16] "Automatic Hidden Shares." 3 Apr. 2002. URL: http://www.winguides.com/registry/display.php/4/ (21 Jan. 2003).

[17] Microsoft Knowledge Base Article – 126025. "How to Disable the Feature That Allows CD-ROMs and Audio CDs to Run Automatically." 13 Aug. 2001. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;126025 (8 Jan. 2003).

[18] "Control the CD-ROM Autorun Function." 17 June 2002. URL: http://www.winguides.com/registry/display.php/6/ (8 Jan. 2003).

[19] Rogers, Lawrence R. "Home Computer Security" 2002. URL: http://www.fedcirc.gov/homeusers/HomeComputerSecurity/#5 (4 Jan. 2003).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced