Global Information Assurance Certification Paper

Home Computer Security – ALL for FREE?
Mark Sutton
GSEC 1.4b
May 3, 2003

Abstract

Is it really possible to protect your home system for FREE, to protect against viruses, worms, Trojans, and hackers? I hear a lot about bugs and vulnerabilities; how do I know where to go for all that patching, updating, and upgrading? And even if I knew, is it possible to keep everything up-to-date without a lot of work? If I only knew what software and hardware was on my system that I needed to protect, then I guess I would have a much better chance of securing my system from the predators on the Internet. Even if I could find all this stuff that I need to better secure my home system, how would I know if it was working? And would these programs be easy to use, even for a beginner like me?

Yes, it is possible to protect your data and system for FREE. There are free virus protection programs, free personal firewalls, and free encryption programs to guard against prying eyes. And, you do not have to stop there. There is FREE software that will tell you all about your hardware and software in and on your system. And there's even one that will tell you if you have passwords on your system that hackers might get. Also, there really are programs out there that will tell you if there is spyware or adware on your system. Many of the tools to be discussed later can be automated. Once everything is secured, there are tools and web sites that will allow you to test your system for FREE and the software and sites will then offer suggestions for making your system even more secure.

Introduction

With a rise in hacking and an ever-increasing number of viruses spreading, it is even more important than ever before to protect your home system and data. There are many systems on the Internet without an inkling of security or virus protection, especially when the trial period runs out on the virus protection software that came with the new system.

A lot of home users say they cannot afford the cost of security software, while many network administrators that are experienced in securing their network would quote the cliché – 'you can't afford not to do it.' Who said you cannot protect your home system from hackers and viruses for free? The purpose of this paper is to expose the home user to a few of the areas and tools that can help to strengthen home security protection for free and increase the user's awareness of their system. Also, we hope to help the home user identify where

patching and updates are needed, and where bugs and vulnerabilities exist. Lastly, the user will be provided with tools and sites that will allow them to test their security and identify weak areas.

Anyone can afford free; I have selected some of the best and most used free security software programs where home users can now afford to protect themselves, their identity, and their data. Because it's ALL FREE! I have also combined these tools with additional free software and sites that serve to heighten system awareness and allow the user to test and evaluate their system. Some of these sites allow for the user to run programs across the Internet to let the user know what their system is divulging or how secure it is.

This paper is geared to the home user. It will focus on FREE tools that can be used on the various Microsoft operating systems to protect the user and their data.

There's no silver bullet when it comes to home computer security. A layered defense is necessary in order to best protect your home system and its data.

In building a more secure layered defense, I will cover the need for virus protection, personal firewalls, strong passwords, and encryption. To heighten awareness, I will cover the need to apply patches and updates, as needed, and to identify bugs and vulnerabilities, too.

With any of the programs that either help to secure your system or provide notification of patches or vulnerabilities, it is very important to automate as much of the protection process as possible. It is easy to forget to do all that needs to be done. It is even harder to remember what has to be updated and what does not.

I will provide the home user with tools that can help to protect their system and educate them to enable them to be more aware of what is going on with their system, as well as provide them with a lot of quality software. Everything is FREE! It's all about awareness. Many people do not realize the degree or extent to which they can protect their home computer for FREE. Also, I will provide some tools and sites that the user can use to test and evaluate their system.

The main goal is to protect your system and the underlying data. Any system can eventually be hacked; your goal is to put up as many layers of defense as possible to get the would-be hacker to move onto an easier system or target.

Security: Virus Protection

Anti-virus software is an important component of a properly protected system and is essential regardless of what your computer is connected to. It does not matter

whether the computer is connected to the Internet, has access to your work network, or is just a standalone computer. You are still vulnerable; it is just the degree of vulnerability at this point. You might think you do not need virus protection if you are not connected to the Internet; even without an Internet connection, it is possible that you could get a virus from a floppy that a friend gave you or one of your family members.

Viruses, worms, and Trojans new and old are constantly running rampant in the computer community. Unfortunately, they do not know any boundaries and can spread and infect any unprotected system. It is of the utmost importance that you have at least one virus protection program on your home computer. The virus protection program should always be running and have the latest signature files to be most effective. Signature files are the files that a virus protection program uses in scanning files for viruses, worms, and Trojans.

After the installation of virus protection software, you need to immediately update the signature files. Your virus protection is only as up-to-date as your signature files are. Often times, the signature files will be weeks or even months out-of-date from off-the-shelf software. Once you get the most up-to-date signature files, keeping the signature files at the latest version is best accomplished by configuring the program for automatic updates. If the virus protection program you are using does not have an automated feature for getting the most current signature files, then you will need to check with the vendor's site at least once a week for new files and consider getting a virus protection program that has the automated update feature. You cannot afford to go unprotected.
These days many viruses are transmitted via email attachments and Internet downloads. This is why great care and caution should be exercised prior to opening any email with attachments or downloading files from the Internet, even if the files are from a trusted source. Trusted sources get infected with viruses all the time. Some viruses use an infected person's email contact list for transmitting a virus. This is why you need to be careful even with trusted sources. If you do not know the sender, it is best to delete the email. If the email from a trusted source looks fishy or the sender has a history of getting infected, then you can always email them to see if they have sent you an attachment prior to opening the attachment. A good rule of thumb is to not open unknown email attachments.

It is important to remember to periodically run an automated, full-system scan with the latest signature files. The main purpose of this procedure is to search for possibly infected files that were not previously discovered. If you are wondering how this could happen, since you have always kept the signature files up-to-date, it is because new viruses are discovered everyday, and you could have a new virus on your system for which past signature files did not detect.

Below are a couple of very useful, free, anti-virus protection programs.

AVAST 4 Home Edition

Avast 4 Home Edition is a popular, full-featured, anti-virus program that is FREE. Avast installs via an installation wizard and is very easy to setup. I took the defaults and within seconds a scan was running, checking the system for viruses. This program requires registration; upon registering for the program, you will be sent via email a license key for the program. This allows for full-featured home use beyond the normal 60-day trial period. After installing and registering the anti-virus software, the next step was to make sure that I have the most up-to-date signature files.

When you first start the program to pull up the anti-virus console, Avast pulls up a simple, 5-step user interface. This interface lays out the steps to do a scan and explains the process in detail.

Some of its features include on-demand scanning, memory scan during application start-up, resident scanner that scans files and email on the fly. Avast can also perform heuristic analysis for protection from new or unknown viruses and/or worms. Other Avast features are the Screensaver scan, which scans the system when the screen saver is invoked, and the Explorer scan that allows the user to right click a file or folder and begin scanning right then and there.[1]

With the default configuration, the automatic update feature checks for new/updated signature files when you are online. At least twice a week, updated files are available; the system will automatically download the necessary files and install them. The system, by default, will also notify you when a program update is available.[1]

Avast 4 Home Edition has some top of the line features and functionality, and it's ALL FREE!

Below is pertinent download information for Avast 4 Home Edition:

Version:	4.0.172
O/S:	Windows 95/98/Me/NT/2000/XP
File Size:	6.21MB
Link:	http://download.com.com/3000-2239-10191261.html

AVG

AVG is another full-featured top of the line anti-virus program that is packed with a lot of features, and it too is free. When you start to download AVG, you must first register the program. Registration will then give you access to the download file, and AVG will also email you the serial number that you need to complete the

installation process. AVG installs via an installation wizard and is very easy to set up once you have the serial number. I took the defaults and within seconds AVG was protecting the system. Just like Avast, the next step was to make sure I had the most up-to-date signature files.

AVG lets the user know the system's status as to which components are active and functional. Many of the features that are in the Avast anti-virus program are in AVG as well. For instance, features such as on-demand scanning, memory scan during application start-up, resident scanner that scans files and email on the fly. AVG can also perform heuristic analysis for protection from new or unknown viruses and/or worms. AVG also has the Explorer scan capability, which allows the user to right click a file or folder and begin scanning right then and there.[2]

With the default configuration, the automatic update feature checks for new/updated signature files when you are online and the files are older than 14 days; however, it can be set to check daily. The system will automatically download the necessary files and install them.

AVG is a very good free anti-virus protection program that would be a good choice to protect your system.

Below is pertinent download information for AVG:

Version:	6.0
O/S:	Windows 95/98/Me/NT/2000/XP
File Size:	5.7MB
Link:	http://www.grisoft.com/html/us_downl.htm

Security: Personal Firewalls

With a continuing increase in the number of users accessing the Internet and an increase in more people doing online financial transactions (taxes, home banking, home shopping, etc.), it is now even more important to protect your system with a personal firewall. Many hackers are looking for financial data or ties to financial data in the form of bank account numbers, credit card numbers, social security numbers, or personal identification numbers.

If you are thinking, why would someone want to hack into my computer – the reasons vary. The intruder could be a curious teenager with some time on their hands. Or, it could be a hacker looking for space for their hacker tools or looking for a system to launch an attack from. Without a personal firewall, you might be their next victim.

Everyone connected to the Internet, regardless of line connection speed, needs a personal firewall. With the many free hacker tools and network administration tools used for bad today, less skilled users can launch an attack against your system.

A good personal firewall should be easy to install, easy to configure, and should protect your computer. One of the most popular and highly effective personal firewalls is Zone Alarm.

Zone Alarm

Zone Alarm is top-notch when it comes to personal firewalls, continually garnering the accolades of many in the computer community. In this day and time of Internet travel, a personal firewall is a necessity. Regardless of your connection speed, someone out there will be trying to scan or hack your system within minutes – if not seconds of getting online.

Zone Alarm includes four interlocking security services: a firewall, an Application Control, an Internet Lock, and Zones.

> The firewall controls the door to your computer and allows only traffic that you understand and initiate. The Application Control allows you to decide which applications can and cannot use the Internet. The Internet Lock blocks Internet traffic while your computer is unattended or while you are not using the Internet, and it can be activated automatically with your computer's screensaver or after a set period of inactivity. Zones monitor all activity on your computer and alert you when a new application attempts to access the Internet [3] (Zone Alarm, CNET).

Installing Zone Alarm is a piece of cake and is educational to boot. Using the installation wizard, I just took all the defaults and it was up and running and protecting my system as soon as I finished the install. There was nothing that had to be reconfigured at that time. Zone Alarm includes a nice informative tutorial during the installation process that explains about the layers of protection, settings, and alerts. The tutorial is set up in such a way that even after the install you can go back and view it repeatedly, if necessary. Also, in the installation routine is a quick user survey that you will need to complete to get through the installation. During the installation routine, you are also given the opportunity to have Zone Alarm notify you when they have updates to their program.

Zone Alarm just keeps giving users more tools and makes it easier for them to protect their system. Alert Advisor is a utility that acts like a security expert. If you are not sure about an alert and its meaning, then you can check with the Alert Advisor and get more information to help you decide what action needs to be taken. In addition to the helpfulness of Alert Advisor, Zone Alarm has an

outstanding Help component that gives understandable explanations that are often supported by graphical representations.

Below is pertinent download information for Zone Alarm:

Version:	3.7.143
O/S:	Windows 98/NT/2000/XP
File Size:	3.57MB
Link:	http://download.com.com/3000-2092-10196007.html

Security: Password Usage

When determining a password to use, always use as strong a password as a site or software will allow. Also, when using or establishing online accounts, use a different password for each account and site. You should not use the same user name and/or password for more than one site. The use of Alt characters can significantly strengthen even a strong password, if the program or site will accept Alt characters. It is not a good idea to allow Internet sites to remember who you are and what your password is so that you do not have to provide a user name and password at the next logon. This is covered in more detailed in the Protected Storage PassView section later in the paper.

A strong password is often defined as having seven or more characters, using a combination of upper and lower case letters, numbers, and special characters. Your password should make use of the tips above; however, it should be easy for you to remember and easy for you to type (prevents shoulder surfing). Your passwords and user names can be stored in password managers, but I prefer to use a tested encryption program and just encrypt my spreadsheet of accounts with corresponding user names and passwords.

Security: Encryption

Encryption is the conversion of data into an encoded form whereby only an authorized recipient should be able to read it. Pretty Good Privacy (PGP) is one of the better-known and widely used encryption programs. PGP is very simple to use and it provides a lot of protection, with very little effort or inconvenience, and is free. The program allows you to encrypt files and email and also do secure deletes in accordance with the Department of Defense standards.

PGP installs via an installation wizard and is pretty easy to setup. Mainly, I just took all the defaults; however, I did have to check that I was a new user, verify that my email plug-in was checked for the email I use, and specify whether or not I had a network adapter. After providing the program with the information above, the system rebooted and entered the key generation wizard. At this point, you

just follow the directions of the wizard and provide a few things like your name and email address. The program will lead you through the creation of a passphrase that you will later use to decrypt encrypted files or emails.

PGP can be used to encrypt sensitive information, such as password lists and other necessary files or emails, etc. Any files that contain confidential information, financial information, account numbers, or other personal numbers should be encrypted.

Password protection programs are nice and can help to keep track of all your passwords. In using a password protection program though, you have to be aware of what encryption algorithm is used to encrypt the data and how strong the encryption is. I recommend the usage of PGP to protect your passwords. A simple password spreadsheet can be created and protected with PGP.

Below is pertinent download information for PGP:

Version:	7.0.3
O/S:	Windows 95/98/Me/NT/2000
File Size:	7.5 MB
Link:	http://download.com.com/3000-2144-4880518.html

Awareness

In addition to creating a more secure environment, it is important for the home user to be more aware of hardware and software on their system. This is especially important in a home environment where multiple people share one computer. Knowing what is installed on your system will aid you in the process of tracking and keeping up with which programs generally need patches or updates. Also, it will make it easier for you to be aware of documented bugs and discovered vulnerabilities.

Delving deeper in the awareness area, and a hot topic these days is spyware and adware and running programs that will detect it. Alongside these programs is a program that will look at protected storage and determine if passwords from various programs are being stored on your system. Even though these passwords are often encrypted, they can be divulged in seconds.

I have used two free software programs that will help you identify all the hardware and software in and on your system. The two products are Belarc Advisor and AIDA32.

Belarc Advisor

Belarc Advisor is a program that scans your system and determines the installed hardware and software details. The output is formatted nicely via a web browser and is very easy to read and decipher. Belarc Advisor installs via an installation wizard and is very easy to set up. I took the defaults and, within seconds, I had a detailed listing of the hardware and software in and on my system.[4]

The hardware information provided includes processor size and type, fixed and removable drives and their capacity, memory size and slots, the type of motherboard, printers, controllers, bus adapters, communication devices, the display, multimedia components and various other devices.

The software information provided includes the operating system with the currently installed service pack, BIOS level, installed Microsoft hotfixes, software license information, and installed software with the appropriate version.

Below is pertinent download information for Belarc Advisor:

Version:	5.1p
O/S:	Windows 95/98/Me/NT/2000/XP/Windows Server 2003
File Size:	611KB
Link:	http://www.belarc.com/free_download.html

AIDA32

AIDA32 is a program developed to give the user an extensive look at their home system from the inside out; AIDA32 does just that. After unzipping the program, the program runs as an executable (no install routine to go through) to scan your system for hardware and software against its large database of software and hardware components. The output of data is in a format similar to the look of Windows Explorer's folder structure. The output is loaded with everything you would want to know about your system and its contents.

Compared to Belarc Advisor, which is good, AIDA32 is a system hardware and software identifier on steroids and then some! AIDA32 is just loaded with detailed information and goes far beyond Belarc Advisor. In addition to the information provided by Belarc Advisor, AIDA32 shows the settings and configuration on any of the hardware components and software installed and has a built-in debug program that can provide dumps as needed on many of the components. Also, it has a report-generation wizard that walks the user through the generation of reports for a system summary, hardware related items, software related items, benchmarking, auditing or a report for everything. If one of those reports does not meet your needs, AIDA32 has a custom report generator where you can pick and choose components. AIDA32 also has a built-

in database update button for keeping the database up-to-date with the latest hardware and software; whereas, Belarc Advisor requires that you check their web site to see if they have an updated version.[5]

Whether you want short and sweet or microscopic details, Belarc Advisor and AIDA32 are both excellent resources and great freebies.

Below is pertinent download information for AIDA32:

Version:	3.4
O/S:	Windows 95/98/Me/NT/2000/XP/Windows Server 2003
File Size:	1.9MB
Link:	http://www.aida32.hu/aida-download.php?bit=32

Awareness: Protected Storage PassView

Protected Storage PassView (PSPV) is a nice little utility that you can run on your system to determine if you have passwords and/or user names stored in your protected storage area, which resides in the registry. Although these passwords are encrypted in the registry, PSPV can reveal them in seconds.

After unzipping the program, PSPV runs as an executable (no install routine to go through) to scan your protected storage for passwords and user names stored there. PSPV can detect and reveal passwords and user names when a user using Outlook Express has selected the option for remembering the password. It can also detect and reveal the user names and passwords users provide when the AutoComplete option is invoked and the user has agreed to allow Internet Explorer to remember their user name and password for a particular web site. Lastly, PSPV can detect and reveal the user name and password for password-protected sites when Internet Explorer is used to access the site and when the special logon box appeared, the user chose to allow the system to save the logon information.[6]

One surprise to many users is the number of passwords stored on their system that they did not realize was there and how easily they could be detected. This is especially important in the day of home banking, home stock trades, online shopping, etc., when the home user is continually passing sensitive information across the Internet and not realizing some it may be stored on their home system. For home users that share a system, but have their own separate logon account, PSPV will only reveal passwords and user names for the current user. There is good news; however revealed, user names and passwords can be easily deleted from within the PSPV program.

Below is pertinent download information for Protected Storage PassView:

Version:	1.31
O/S:	Windows 95/98/Me/NT/2000/XP
File Size:	20KB
Link:	http://nirsoft.multiservers.com/utils/pspv.html

Awareness: Spyware and Adware

Spyware is a smaller program written and placed in a larger program designed to provide advertisers or other interested parties with certain information the program gathers. Adware is software that has had additional code added to the program to enable pop-up windows or other advertising techniques. Spyware and Adware are sometimes included in freeware or shareware programs to help the developer recoup programming and development costs by providing others with pertinent information about the user, their system, and/or where they have been on the Internet. It should be noted that by deleting the ad-modules of some programs that contain spyware and adware, the program can be rendered non-functional.

Ad-aware

> Ad-aware is THE award winning, multi-trackware detection and removal utility (designed for Windows 98 / 98SE / ME / NT40 / 2000 / XP Home / XP Pro) that will comprehensively scan your memory, registry, hard, removable and optical drives for known Datamining, aggressive advertising, Parasites, Scumware, Keyloggers, selected traditional Trojans, Dialers, Malware, Browser hijackers, and tracking components [7] (Ad-aware, pg.1 para.1).

In addition to all the functionality above, Ad-aware has a Webupdate module now integrated into the program that allows for the reference file to be updated at the click of a button; however, the free version does not check for updates automatically. The reference file is comprised of many signatures that are compared to files on a user's system and are updated on a regular basis. Just as easy as updating the reference file is, using Ad-aware's installation wizard is a snap too. It can be installed in just a couple of minutes, taking the default settings and did not require any registration. Once you have Ad-aware installed, it has a lot of useful features-one being a help section that is searchable and another being a very useful manual.[8]

After installation, the Scan module has a default scan setting mode, which can get you up and scanning immediately for adware and spyware until you have time to explore the scan options and other modules. After running a scan, a report is automatically generated that lists a summary of the potential spyware and adware software found. You can then select what you want to delete. The

files that are found are quarantined until you determine they need to be deleted or that they are fine and can be restored.

Below is pertinent download information for Ad-aware:

Version:	6.0
O/S:	Windows 95/98/Me/NT/2000/XP
File Size:	1.45MB
Link:	http://download.com.com/3000-2144-10186632.html

Spybot Search & Destroy

The Spybot Search & Destroy (Spybot S&D) program is like Ad-aware on steroids. "SpyBot – S&D searches your hard drive for so-called spy- or adbots; little modules that are responsible for the ads many programs display. But many of these modules also transmit information about your surfing behavior and more to the net. If Spybot – S&D finds such modules, it can remove them."[9] Additionally, Spybot has the capability to remove the tracks of cookies, started programs, last visited web sites, and opened files.

Spybot S&D's install wizard makes installing the program very easy and quick. The software can be installed, taking the defaults, and did not require any registration. Once Spybot S&D was installed, it was ready for action and ready to go hunting. I first ran Ad-aware to clean up the adware and spyware on a system, then I ran Spybot S&D and many additional adware and spyware components were identified for my review. Spybot has an easy mode and an advanced mode. As you would expect, the easy mode is configured with default settings to get you up and scanning as soon as possible after install. Whereas, the advanced mode allows for many scan and configuration changes to accommodate very detailed and specific scans. Both modes make it easy for the user to download the program's latest update files prior to the first scan. The program has a convenient update button on its' interface. Within the advanced mode, there is a setting that allows for automating the update process via the Webupdate component and the program can be configured to look for updates while online.

New to Spybot S&D version 1.2 is an immunization option, which allows for spyware to be blocked automatically during the download process. Thus, the spyware is not even making it down to your machine to begin with. Also noted within the program, is a tutorial that provides a lot of useful information about running scans and interpreting the results, all complete with easy to follow screenshots.

Spybot S&D should be an essential part of your system security to keep adware and spyware off your system and limit what others can find out about your system.

Below is pertinent download information for SpyBot Search & Destroy:

Version:	1.2
O/S:	Windows 95/98/Me/NT/2000/XP
File Size:	3.5MB
Link:	http://download.com.com/3001-2144-10194058.html

Awareness: Patches, Updates, Bugs, Vulnerabilities, Alerts/Notification

With the installation of software, comes the need to apply patches, updates and/or make configuration changes. Some of the reasons to make changes to the software programs or an operating system (OS) after installation is because of insecure default configurations, missing patches and updates or service packs, incorrectly configured components, and weak default passwords.

Patches and updates should be applied as soon as possible after the software has been installed to help ensure that it is up-to-date. The patching and updating does not stop there. You have only just begun on the road to keeping another program patched and updated; and probably for only a short time, you are not as vulnerable to an attack. Hackers are continually trying to break applications and operating systems. This is why patching and updating is a continual effort.

One thing to consider when purchasing software is to contact the vendor about its patch/update policy and their method(s) of notification when patches, updates, or upgrades are available. Many software companies have an email list that you can sign up for to let you know when patches, updates, or upgrades are available. Often a nuisance, but it is essential that you register all the software that you install on your home computer. This allows the vendor to contact you, usually via the email address you provided at registration, with patches, updates, vulnerabilities and upgrades.

A good place to start is to make sure your OS has all the latest patches, updates, and service packs. You should consider the Windows automatic update client that can be configured to notify you when updates are available. The update page scans your system to determine what bugs and vulnerabilities exist that need to be patched or updated since the computer was setup or since the last scan.

Additionally, you will want to sign up for email lists for notification of service packs, patches, updates, hot fixes, and vulnerabilities for your OS. Since this paper is covering Microsoft operating systems you will definitely want to

subscribe to their email list. It is also a very good idea to have other sites notify you other than Microsoft related to the OS. Sometimes, Microsoft can be a little slow about making the public aware of a bug or vulnerability in one or more of their operating systems.

When it comes to application programs, you need to register the software program and/or visit the software developer's web page. Some software developers do a pretty good job of keeping registered users up-to-date. There are independent sites that collect and post bugs and vulnerabilities that have been identified in the computer community. Bug sites, as well as a lot of security sites, document the latest bugs and vulnerabilities and many often offer the level or degree of seriousness of the vulnerability and provide the types of operating systems or applications that are susceptible. If you use Microsoft Office suite, there is an update page. While checking the Microsoft operating systems page, check the Microsoft Office page, as well.

The more mainstream the application is, the more you should be able to rely on the various free email notification services. If the program is little known, and it is a program that you have to have, it is a good idea to make sure you have registered the program with the software company and check its site for patches, updates, bugs, or vulnerabilities that they have made public.

Alerts or notifications are a big part of the overall awareness process. The alerts come in the form of security alerts, virus and hoax alerts, patches, bug fixes and vulnerability alerts. The best process to follow to find out about these alerts is to subscribe to numerous email alert services and mailing list services. It is a good idea to sign up for as many reputable ones that you can find. This is to better protect you in case one or more of your sources does not alert you in a timely manner or worse – not at all. This is the automation of the process I mentioned earlier. It is also a good idea to visit your resource sites on a regular basis to see if valuable services are available or if there are changes that you need to implement to ensure you are notified.

When you receive a notification via email, I would recommend that you not just blindly apply each and every patch or update. You need to read what the patch or update does. If you cannot determine if you should apply a particular patch or update, consult one or more of your tech savvy friends or review some Internet sites that explain the patch.

For software and/or vendors that do not have an automatic update mechanism, you will need to establish a time when you will visit the web sites of your software vendors to check for patches, updates, vulnerabilities, and upgrades, or visit sites you have identified that list all kinds of programs.

The last word on patches, updates, etc., is – automate, automate, automate. Have all the alerts sent to you that you can, since most home users do not have a lot of time to devote to searching for what needs to be patched or updated.

Below are some very good sites for identifying and providing virus alerts, needed patches, etc.

Note: Some URLS may wrap.

Virus Alerts – email notification:

Avast32

http://www.asw.cz/vpsinfo.htm

AVG

http://www.grisoft.com/html/us_alert.php

Panda Software

http://www.pandasoftware.com/register.asp?CodigoProducto=99&TipoLead=2&TipoUsuario=2&Tipo=1&Ref=ww-SUSCRIP&Idioma=2&Country=us&sec=about&Lst_6=true&Lst_5=false&Lst_7=false&Lst_8=false

McAfee Security

http://vil.nai.com/vil/content/alert.htm

Computer Associates

http://esupport.ca.com/index.html?VirusInfo

Security, Patches, Updates, Bugs and Vulnerabilities:

CERT Coordination Center

http://www.cert.org/contact_cert/certmaillist.html

SANS

http://www.sans.org/newsletters/ (registration is free, but required)

http://www.sans.org/top20/ (registration is free, but required)

Microsoft Security

http://www.microsoft.com/security/security_bulletins/decision.asp

Computer Incident Advisory Capability (CIAC)

http://ciac.llnl.gov/ciac/

SecurityFocus

http://www.securityfocus.com/archive

NTBugtraq

http://www.ntbugtraq.com/

HackerWhacker (has a beginners section)

www.hackerwhacker.com

Scans:

Microsoft Windows Update Scan

http://v4.windowsupdate.microsoft.com/en/default.asp

Microsoft Office Update Service

http://office.microsoft.com/productupdates/

Testing – System Review

You have not only been exposed to numerous tools that will help to secure your system and add layers of protection, but also made aware of tools that will help to increase your system awareness. With that said, we will now look at a few sites that provide tools and/or programs, which will provide immediate feedback on the security of your system and/or where you might be vulnerable to hackers and the like. These tools and programs should be run against your system on a regular basis for two reasons. One reason is that these tools and programs are always being updated; and another is the degree of security needed on your system changes day-by-day and week-by-week. Unfortunately, security is not something you can setup and forget. It is important to take advantage of as many automated tools as possible for keeping the product up-to-date or, at a minimum, have the vendor notify you of changes and/or updates.

Below is a selection of sites and tools (with description) that are free to test and evaluate your system.

Microsoft Baseline Security Analyzer (for Windows NT/2000/XP) scans for vulnerabilities for Windows, SQL, and IIS. It also scans for security updates and weak passwords.[10]

Link: http://www.microsoft.com/technet/security/tools/Tools/mbsahome.asp

AuditMyPc.com tests your firewall and performs a security audit. Some of the more specific things it tests for are browser and spyware vulnerabilities and ports commonly used by viruses and Trojans. If your system is not properly configured, these tests can read information copied to your clipboard, open your CD-ROM drive, track your Internet activity using SuperCookie, and detect open ports commonly used by virus and Trojan programs. This site tells you how to fix the vulnerabilities it finds.[11]

Link: www.auditmypc.com

EICAR (European Institute for Computer Anti-Virus Research) is a site that allows you to download a safe virus to determine if your anti-virus protection is working. If your virus protection software is working, then it will catch the test

virus. If not, you need to review the configuration of the anti-virus program that you are running or get a new one.[12]

Link: http://www.rexswain.com/eicar.html

Gibson Research Corporation has two products to test your system. Both are listed in the 'Hot Spots' section on their main page – ShieldsUP! and Leak Test.

ShieldsUP! checks the security of your machine using two components. **Test my Shields!** attempts to connect to the hidden Internet server in your machine. **Probe My Ports** attempts to connect to standard, well-known service ports.[13]

Leak Test tests your firewall to see if a virus or malicious Trojan can trick it.[14]

Link: http://grc.com/intro.htm

If your system is not adequately protected and secure, some of the things these programs and sites divulge and do are alarming.

Conclusion:

I have tried to provide a wide array of FREE software programs and sites to strengthen your system security, heighten your awareness, and allow you to test your system. Areas to note are:

- Virus Protection
- Personal Firewalls
- Passwords
- Encryption
- Hardware and Software Inventory
- Protected Storage
- Spyware and Adware
- Patches, Updates, Bugs, Vulnerabilities, Alerts/Notification
- Testing Sites and Tools

I have provided many choices in the areas above. As a result of all the choices, the user has a better opportunity to pick the ones they are most comfortable with and that match the user's skill level.

By implementing the FREE tools discussed and some of the other security steps in this paper, the home user will better be able to protect their home system against viruses, unauthorized access, protect against attacks, and better secure sensitive data and, at the same time, be more aware of their system and where to test it.

Although everything discussed above has been FREE, you need to educate yourself on the products discussed above and determine if they meet your security needs. If not, there are a lot of other FREE programs out there in each area. Another comparison that you will want to make is to compare the FREE software to programs that require a fee for the usage of a program. You have to ask yourself, are the additional features worth the money for the level of security you feel you need for the environment in which you compute?

It should be noted that the resources mentioned above are recommendations only; however, many are very good programs and would be a great asset to your security posture and help to develop a layered approach to security with an emphasis on awareness.

References (Some URLs may wrap)

[1] ALWIL Software, CNET. "Avast 4 Home Edition 4.0.172." Version 4.0.172. URL: http://download.com.com/3000-2239-10191261.html (16 April 2003).

[2] Grisoft. "AVG AntiVirus." Version 6.0. URL: http://www.grisoft.com/html/us_downl.htm (16 April 2003).

[3] Zone Labs, CNET. "ZoneAlarm 3.7.143." Version 3.7.143. URL: http://download.com.com/3000-2092-10196007.html (4 April 2003).

[4] Belarc. "Belarc Advisor." Version 5.1p. URL: http://www.belarc.com/free_download.html (22 April 2003).

[5] AIDA32. "AIDA32." Version 3.4. URL: http://www.aida32.hu/aida-download.php?bit=32 (22 April 2003).

[6] NirSoft. "Protected Storage PassView." Version 1.31. URL: http://nirsoft.multiservers.com/utils/pspv.html (20 April 2003).

[7] Ad-aware. "What is Ad-aware?" Ad-aware 6.0 Help section (2003): pg.1, para.1.

[8] Lavasoft, CNET. "Ad-aware 6.0." Version 6.0. URL: http://download.com.com/3000-2144-10186632.html (16 April 2003).

[9] EJRS."Spybot Search & Destroy." Version 1.2. URL: http://ejrs.com/spybot/ (23 December 2002).

References (Continued)

[10] Microsoft. “Microsoft Baseline Security Analyzer.” Version 1.1. 2 December 2002.
URL: http://www.microsoft.com/technet/security/tools/Tools/mbsahome.asp
(14 April 2003).

[11] Maurer, James. “AuditMyPC.com.” URL: www.auditmypc.com (14 April 2003).

[12] Swain, Rex. “EICAR Test Virus.” 29 May 1999.
URL: http://www.rexswain.com/eicar.html (14 April 2003).

[13] Gibson, Steve. “Shields UP!!”
URL: http://grc.com/intro.htm (15 April 2003).

[14] Gibson, Steve. “Leak Test.” Version 1.2. 2 November 2002.
URL: http://grc.com/intro.htm (15 April 2003).

Last Updated: July 23rd, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
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
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
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
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 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
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
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
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS 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
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor