Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Simple Security for Windows

Security as it relates to Information Technology, computers, and servers has rapidly left the corporate world behind so imagine what it has done to the average user. In the corporate world we are doing vulnerability assessments and pen tests. We are running sniffers and intrusion detection. Patch management and virus definitions have become a way of life. Where does this leave the average user? The answer is very simple. They either pretend they know what you're talking about as you tell them what they need to do to secure their equipment, they give you a blank stare and go on in blissful ignorance, or they start turning purple and have an aneurism right before your eyes. This paper will provide the day to day user with step by step instructions to harden their PC. We will bring all those security terms down out of the ether and show the average individual how to stop walking through the battlefield of the internet in nothing but a Speedo.

"Simple Security for Windows" includes the elements listed below. Many security discussions will rely on one or two when in fact you can't leave anything out.

Security Steps & Categories

1. Don't use simple or obvious passwords.
2. Protect your computer against viruses & worms.
3. Apply all security patches and service packs.
4. Subscribe to industry security bulletins.
5. Load, learn, and use a personal or hardware firewall.
6. Load and run Ad-Aware to remove spyware.
7. Scan your PC using the Microsoft Baseline Security Analyzer.
8. Specific tips for Microsoft XP and 2000 operating systems.
9. Enable auditing and use the Event Log.
10. Understanding security templates & policies.
11. Using the Encryption File System.
12. How to permanently delete files.
13. Best practices for the use of Wireless Access Points.

Purpose Statement

The purpose of this document is to provide average users who don't understand all that, "Geek-Speak" with a simple reference that anyone can follow to secure their personal computer and the data contained thereon from all but the most dastardly attacker's, viruses, or worms.

Created by submitted on 11/10/2003 1:09 PM

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Passwords

Almost every time a password is compromised it is because there was an account with no password or a weak password on one of the accounts. If you are a home user this means your email password or your logon password. For the corporate user this is the password that was given to you by your network administrator. Some corporations control the strength of the password. If your corporation provides guidelines then just follow them and you should be okay. If not then you should consider the following.

Don'ts

- Don't use the name of a family member, pet, favorite college sports team etc… These can be easily guessed by anyone who knows you well. I can't tell you how many times I have sat down at a PC and looked on the back of the pictures on the desk and seen a cute little picture labeled Fluffy the dog and presto, Fluffy is the password.
- Don't use your phone number, house number, birthday, or anniversary. These are the first things a person will try to crack your password.
- Don't use a word out of the dictionary in any language. The programs that are used to crack passwords go through a dictionary trying every word until it cracks. The more elaborate dictionaries use medical terms, foreign languages, and even popular phrases like, "Take me out to the ball game".

Do's

- Use 8 characters or more
- Use a combination of letters, numbers, and special characters.
- Use a combination of upper and lower case.

To set your password on Windows 2000 or XP, hit CTRL-ALT-DEL and select the "Change Password" option. In older Windows operating systems go to the Control Panel and click on the password icon. The [1]IT team at Duke University has an excellent reference about choosing proper passwords and their relative strengths and weaknesses.

Anti-Virus, Viruses, & Worms

A computer virus is a malicious code, script, or program that will cause an undesired or unsolicited event to occur on your computer or email. A virus requires interaction from a user such as clicking on or opening an attachment or clicking a malicious hyperlink. Some examples of what a virus could do, can be taken from recent events. For example the, [2]"I Love You" virus arrived in email, if opened, it would overwrite files on your hard drive, attempt to download and install a password stealing program that would send the infected PC's passwords to a mailbox. It would also mail itself back out from the infected PC to infect other PC's. A virus requires that a user click something or take an action of some kind and is therefore not the current favorite of attackers.

Created by submitted on 11/10/2003 1:09 PM
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Recently Worms have been the preeminent method of attack. Worms propagate very quickly and can even affect the entire internet by consuming bandwidth. Worms are a common method of attack because they don't require a user to do anything. A worm is also a script, malicious code, or combination of these that causes an undesired or unsolicited event to occur. The key difference is that the worm does not require a user to be involved. A worm infects a PC through an unpatched vulnerability or an exploit that compromises or bypasses normal PC operation and security.

Viruses can be mitigated by Anti-virus software and all computers should be running a reputable Anti-virus program. Anti-virus software is only as good as the information it has, so make certain that you keep your definition files up to date. Definition files are files that tell the Anti-Virus program what to look for in order to detect and remove the currently know viruses. As new viruses are discovered definitions are updated to detect them. Your manufacturer's website will tell you how to update the virus definitions for your Anti-Virus Software.

It is also important to keep track of which Anti-Virus software is the most effective. The [3]Virus Bulletin website is an excellent source to determine which Anti-Virus vendor has the best record for detecting viruses. Choose an Anti-Virus vendor, purchase, install, and update this software to protect your PC from viruses.

Worms are much harder to protect against. The best way to protect you PC against worms is to follow *all* the instructions in this document paying strict attention to patch management and the Microsoft Baseline Security Analyzer. The only way to protect your PC against worms is to keep up with and mitigate vulnerabilities as they are discovered. Many worms can only come through a firewall on specific ports. If you have high speed internet access you should purchase and install a hardware firewall and follow the instructions below for a software firewall for defense in depth.

Patch Management

[4]Microsoft has provided a tool that will allow you to keep all of your security patches and hot fixes up to date. The Windows Automatic Updater can be configured to notify you when new patches are available or even to download and install the patches for you on a schedule that you specify.

[5]Keep Up To Date with Microsoft Security Fixes

The Windows Automatic Updater can sometimes install a patch that you don't want. It only gives a user limited control over what gets applied. Microsoft offers the Windows Update site. This site is more robust than the Windows Automatic Updater, because it offers optional patches and driver updates that don't necessarily need to be applied to all PC's and it gives a user total control over what patches and drivers get installed. PC's often need updated software that tells them how to interact with their hardware better. These are called drivers. As new drivers are released and are tested and approved by Microsoft they will be available at the Windows Update Site. The Windows Update Site also has a searchable database of all updates and drivers called the Windows Update Catalog. This can sometimes be used to find outdated or obscure patches that don't show up automatically. It is also useful for downloading patches that you have already installed, but may need to reapply. Once you scan your computer and apply a given patch it will not show up again so be aware that the catalog exists and can be used to search for any patch.

Created by submitted on 11/10/2003 1:09 PM
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

[6]**Subscribe to Microsoft Security Bulletins**
[7]**Subscribe to SANS Security Newsletters**

Microsoft & SANS release bulletins from time to time warning of security flaws and exploits as they are discovered. Click on the links above and you can subscribe to these free email notification services. When a critical vulnerability is discovered or patches are needed you will be notified.

Firewalls

A personal firewall is like a full time traffic cop with arrest power protecting your computer. It is on duty all of the time watching access in and out of your computer. Your computer is constantly communicating with applications, devices, and other computers through the internet. It does this via transport protocols, ports, and the OSI Network Layers. Many of you have no idea what I just said so let's take a moment and explain the personal firewall. Think of your computer as a very busy post office. There are letter carriers (transport protocols) going in and out all of the time. Each type of letter that they carry has a different destination within the building and a specific route through specific doors to get there (ports). Without a personal firewall any letter carrier (transport protocol) can go through any door (port) to get its letter or package (potentially a virus or Trojan Horse) into the building. The personal firewall locks all of the doors (ports) and stops each letter carrier and inspects the contents of their letters (stateful packet inspection) and only lets through approved traffic. What this means is that your computer at home without a personal firewall will let in just about anything if you or some program has left the door open. This is especially true if you have always on high speed internet such as DSL or Cable. A personal firewall closes those doors and forces you to choose, through the firewall program, what to allow and what not to allow. The [8]Zone Alarm Firewall by Zone Labs is free for personal use and will protect your PC from unauthorized traffic. Click on the icon to load the free version and get step by step instructions.

Zone Alarm Instructions

There are two types of firewall's to consider for home use. Zone Alarm is a software firewall and is a very good option for home users. High Speed internet users of DSL and Cable should also consider a hardware firewall. A hardware firewall is installed between your cable router or DSL modem and your PC. Depending on the model and brand of firewall that you install you will have extra features not found on most software firewalls such as Virtual Private Networking or the ability to create conduits. Advanced users can use VPN to connect to their home computers securely from work or while out of town. A conduit is a feature of some firewall's that allows you to allow a specific type of traffic only to specific PC's. Using this feature you can allow email traffic (SMTP or POP3) to go to a mail server but no other PC's. If you have multiple computers you can buy a hardware firewall that has a built in switch. If your equipment has this feature you can connect and protect multiple computers for file sharing, internet access, and gaming.

Created by submitted on 11/10/2003 1:09 PM
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Spyware

A new problem for computer users today is spyware. Spyware is software on your PC that tracks your activities or the information you enter into web pages and reports back to some host company or individual. Some examples of spyware are listed below.

Browser Parasites or Ad–Bots

A browser parasite is a program that attaches itself to Internet Explorer and then tracks and reports your activities and personal information that you enter on web pages back to a host company.

NOTE - Not all browser parasites are dangerous or malicious, many are completely harmless. Most are collecting innocent demographic data. It is the lack of disclosure and the fact that many cannot be uninstalled that causes the most concern.

How do I get browser parasites or ad servers on my PC? - Many freeware programs and shareware programs make their money through advertisers. (Nothing is really free) When you download and install freeware and shareware it often loads browser parasites or add servers. Install and run Ad-Aware using the instructions below to remove these parasites.

What are some indications that I have a browser parasite?

- Your internet connection becomes very slow. One of the causes for internet slowdowns can be ad-bots consuming bandwidth.
- You are receiving unsolicited emails. Ad-bots collect information that you enter into web forms. This information can be sold as sales leads to marketing firms. Email addresses are often captured.
- You are seeing more pop up advertisements than usual. These are the advertisement web pages that open without any action from the user.

Gator is one of the more notorious and pervasive examples of an Ad-Bot or browser parasite. It tracks and captures many of your web activities and sends them back to the advertisers and host companies. Click on the icon to load the free version of Ad-Aware and get step by step instructions for its use.

How to Load and Run Ad-Aware

Microsoft Baseline Security Analyzer

Microsoft has provided a tool that is geared toward the average computer user. [9]The Baseline Security Analyzer or MBSA will scan your system for many of the vulnerabilities discussed in this document. It will provide a report that tells exactly what is needed to help secure your PC and links that show exactly how to do it. It doesn't cover all of the bases we are covering in this document, but it certainly gets most of them. I highly recommend that you download, install, and run this tool regularly. MBSA will check the following systems: Windows NT 4.0, Windows 2000, Windows XP, Internet Information Server (IIS) 4.0 and 5.0, SQL Server 7.0 and 2000, Internet Explorer (IE) 5.01 and later, and Office 2000 and XP.

Created by submitted on 11/10/2003 1:09 PM

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

XP and Windows 2000

Set an Account Lockout Policy

To prevent someone attempting to guess your password (through an automated process called a dictionary attack); you should configure an account lockout policy. Such a policy will lock an account until the Administrator unlocks it. If an attacker is using a password cracking utility, the utility will repeatedly try to guess the password. This is accomplished by using guessing algorithms and or dictionaries files. The password cracking utility attempts to log on using every word in the dictionary file. If an account lockout policy is defined then the account will be locked and will need to be unlocked by an account with the necessary privileges or it will automatically reset in a specified amount of time. This either completely stops the cracking attempt or vastly increases the amount of time necessary to go through the dictionary attack. Note that the Administrator account can only be locked for remote access, you can always physically log on to the computer as Administrator. Here are some detailed instructions from the folks at Duke IT Security. [10]**Set an account lockout policy**

Disable Unnecessary Services

Windows 2000 and Windows XP come with programs and functionality loaded by default that is often not used by average users. This can include but is not limited to the following list: Internet Information Services, File Transfer Protocol, Telnet, SMTP, and others. The average user doesn't even know what these services are or why they are used. The services listed above are some of the most commonly exploited and vulnerable programs in the Windows operating system. These programs will not be needed on most home PC's and should be disabled. The IT team at Duke University has [11]simple instructions for disabling these services.

Disable the Guest Account

You may not know it, but your computer happily invites any passerby on the information super-highway to come on in and have a look around. Being the gracious and proper host it doesn't show them everything by a long shot. The bedrooms and other private areas are off limits, but what burglar needs to see the whole house in order to, "case the joint." All of this is done via the Guest Account which is an account on your PC that allows anonymous access. In some ways it could be argued that this is beneficial. In a corporate environment it allows tools and utilities to see certain public information about your PC with no password. More often than not there is no legitimate reason for this. The guest account should be disabled. Later in this document when you learn about the Microsoft Baseline Security Analyzer, it will show you how to disable the guest account.

Created by submitted on 11/10/2003 1:09 PM
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Disable the Default Shares & Null Session

By default, Windows allows access to all the drives on your computer and other information such as lists of users and groups, lists of machines, lists of shares, and some registry keys. This is done through default shares and the use of something called a Null Session. A Null Session is a communication between systems that is established without a password. An excellent explanation of null sessions can be found at [12]http://rr.sans.org/win/null.php . When a null session is enabled on particular resources or shares this can allow unauthorized access without the use of a password. If you are running a single PC at home all of this can be handled by stopping the server service. If you are using your PC at work or in conjunction with other PC's, servers, or remote applications disabling this service will cause problems. The Berkley Lab has good information on [13]how to handle default shares. Brown University CIS department is an excellent resource for [14]combating null sessions.

Create a user account

A common problem among the user community today occurs when a user doesn't create an account. They simply log on as administrator and do their daily work. The problem with this is that any exploit that runs in the context of the logged on user is now going to run as administrator. The argument has been made that if the user account is not an administrator then I will be unable to load certain programs. If your account is not an administrator simply hold down shift and right click the icon. In the list you will see, "Run As". Click run as and type your credentials and away you go. Another reason to create user accounts and use them instead of the administrator account is for the purpose of logging and auditing. If multiple users use the administrator account then it will be impossible to tell which user performed a certain action when referring to the logs. Step by step instructions for creating a user account can be found at [15]Duke University's IT page.

Windows 2000 and XP can also be configured to logon automatically. When you turn on the computer it goes straight into the operating system with no logon required. This allows anyone with physical access to the computer to manipulate the system in any number of ways. If you follow the instructions in the Security Policies and Templates section below to ensure that all users are required to press Control-Alt-Delete and type a username and password to logon.

Consider Disabling Raw Sockets

According to [16]Steve Gibson of GRC.com Raw Sockets can be used to launch Denial of Service and Distributed Denial of Service attacks that would be untraceable. If your PC was infected by a worm such as Nimda, it could then launch untraceable raw socket attacks on other PC's. By disabling Raw Sockets you reduce the risk that your PC can be used by someone else to launch malicious denial of service attacks. A tool to test and disable raw sockets on your PC can be found at [17]GRC.com .

Created by submitted on 11/10/2003 1:09 PM
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Auditing

Windows XP, 2000, and NT have the ability to track three categories of actions taken on the system. These categories are System, Application, and Security. The catch is that none of these items is tracked by default. All systems should have auditing turned on and the event log properly configured. If a user successfully attacks a system and gains access it will almost always be detected in the event log. Even if a user is authorized to be on the PC, but takes an action while logged on that is harmful to the organization or individual who owns the PC it can be tracked. Auditing the Application and System section of the event log is also very helpful in troubleshooting system problems. The system and its applications report everything from errors to routine information in these logs. All users should become familiar with the event log. Microsoft has provided instructions for auditing at the following URL: [18]http://support.microsoft.com/default.aspx?scid=kb;en-us;300549#2 Auditing is probably one of the most complicated things that we have discussed so far. If you feel yourself getting a little bit lost go to the next section. In the policy section I will show how you can further secure your PC and enable auditing with a few mouse clicks.

Security Policies and Templates

As we continue to work with the security of your PC we need to discuss security policies and templates. If what we have already discussed wasn't enough to let you know that PC security is no longer as simple as we might like, hold onto your hats because there is a whole other world of systems security in policies. If you use your PC at work you shouldn't have to do anything, because *ideally* the network administrator of a secure domain will set the policies for all of the systems in such a way that when each individual logs on the policies set by the administrator are applied to it. This is called Group Policy under Windows 2000 and when each user logs on they will receive the default domain policy and any other policies related to their location within the network.

How do you know what policies are set on your PC and what they do? If you are at work you should look but not touch if you are concerned that this could be an issue. If you find problems in a corporate environment report them to your network administrator. To check the level of security of your policies you can go to the Center for Internet Security and [19]download benchmarks that will test your computer against industry standards agreed upon by the [20]members of CIS. These benchmarks require some expertise to understand and remediate the results.

In Windows 2000 and XP I recommend that you go to the control panel in your PC and click on Administrative Tools then click on Local Security Policy. This will open the Local Security Policy snap-in for the Microsoft Management Console. Click on action, then import policy, then choose hisecws.inf, click open, and then click action & reload. This will load the High Security Workstation template. If you have any problems with your PC after loading this template repeat the process and choose securews.inf or as a last resort compatws.inf to get your PC working. If you search the web many other agencies publish their recommended INF files. Research the agencies and pick the one you prefer. The Center for Internet Security linked above has the best of the best.

Created by submitted on 11/10/2003 1:09 PM
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Encrypting File Systems in Windows 2000 & XP

At this point we have gone through more than most of us ever wanted to know about how to protect our PC's; so we are doing pretty good right? If the PC remains in your possession handcuffed to your wrist or desk at all times it is probably pretty secure from viruses, hacking, spying, patch vulnerabilities, and all those other nasties we have discussed. What happens if someone snatches your laptop from you at the airport or you accidentally leave it somewhere? All of your hard work and data is protected by one complex password (if you've been following instructions) or the name of your favorite football team if you haven't. Even if the person that finds or steals your laptop can't crack your password, they can always use a boot disk and some other tricks of the trade to get your data. It is frightfully easy to get the data off of a laptop that is only secured by a Windows password. This is where encryption can enter the scene.

Windows 2000 and XP have the Encrypting File System built in. Without getting into a highly technical discussion of encryption; the basic gist of encryption is that your data is scrambled with a secret key and a password. Encryption has varying strengths. It is recommended that you always use 128 bit or higher. Encryption usually consists of something you know (Password) and something you have (Encryption Key). Windows 2000 and XP encryption is not the best because you don't have control of the key unless you export it when the computer is not in use. The advantage of EFS is that it is free and it will prevent someone from getting your data with a boot disk if you follow the best practices in the article from Microsoft linked below. If an individual gets your password EFS will not help much so remember to use a complex password and don't share it or give it to anyone. Please see the link for more detailed information and instructions from Microsoft for configuring EFS.

[21] **Best Practices for Encrypting File Systems**

When it comes to file encryption another well know program that I recommend is PGP. PGP stands for Pretty Good Privacy, and although the name may sound funny pretty good privacy is exactly what it provides. I would call it PDGP for Pretty Darn Good Privacy. Many rumors abound that NSA and others have cracked PGP, but I have never seen definitive proof of this and in my opinion if you use PGP your data will be encrypted strongly enough to prevent all but the most aggressive and well funded attackers. What that means is that you and I who probably don't work for the CIA can feel pretty secure about PGP. PGP goes beyond EFS and many other encryption programs. In some version of PGP it includes file encryption, file wiping, and a firewall. PGP interfaces very well with Outlook and other email programs. EFS does not allow encryption of email so get PGP to secure your email communications. PGP can use a variety of algorithms and bit strengths: Cast, AES, Twofish, and TripleDES are some of the options. To get started with PGP click on the enclosed document icon below. PGP has a free version for non commercial use. Please follow all licensing guidelines and export restrictions for PGP.

PGP Instructions

Created by submitted on 11/10/2003 1:09 PM

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

More information and Security Links for Older Operating Systems

If you are still using one of the older Windows Operating Systems please consider upgrading to XP Professional or Windows 2000 as soon as possible. They are much more secure.

[22]**Microsoft Security links for Windows 9X, SE, ME Desktops**

Permanently Delete Files[23]

[24]If you delete a file is it really gone? If you have ever had to recover a file you may be aware that they can often be recovered. What if you deleted a file several years ago or you have run defrag or installed programs since it was deleted? Is it gone? What if you have even completely reloaded the computer? The answer is sometimes yes and sometimes no. That answer isn't much help. The bottom line is that many files can be recovered years later even after all of the circumstances above have occurred. It is not always easy and it can require special software, hardware, and expertise, but it can be done.

So why is this an issue? Let's say that you have a PC that has patent information on it that is very valuable or perhaps your work is very secure or confidential and you want to sell your old PC and buy a new one. Can the person who buys your PC get any of your data? Yes, if they have the equipment and skills they can almost always get some of your data. The operative question then becomes how do I prevent this. It is necessary to overwrite the data and delete it several times to ensure that it is completely gone and unrecoverable. When you delete a file in most systems it is like removing the index tab from a file in a filing cabinet. That file folder (disk space) is now available for new content if needed, but until someone takes out the old papers (data) and throws them away the information is still in the filing cabinet. It is not easy to find because the index tab is gone, but all of the information is still there. This is an analogy of what happens when you delete a file without using a deliberate method to ensure that it is irrevocably gone.

The art of getting these files and other similar information back is part of Computer Forensics. In order to remove the files permanently I recommend [25]CyberScrub. There are free tools available, but they are not recommended for something this critical. Take the time and investigate and purchase a tool that will: Overwrite the data with ones and zero's, perform multiple passes, exceed DOD standards, and prevent Hardware recovery. Many of these tools don't wipe the swap disk and don't have any facility to delete locked files like index.dat or cookies. It is also important to wipe the free space which contains the residue from deleted files. CyberScrub meets all of these recommended requirements.

Created by submitted on 11/10/2003 1:09 PM
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Wireless Access Points & Security

Let me start by saying that in my humble opinion there is no way to completely secure a wireless network. GCN.com has excellent information regarding the [26]dangers of wireless networking. Many will argue that there is no way to completely secure any network and there is definitely some truth to that. Some inherent weaknesses only apply to wireless. One key difference is that there are no hardwired network jacks on the outside of your home or corporate office that a hacker can walk up to and use. If you are using wireless then you have extended your physical security outside your building. Even though there is no tactile element your network is now floating around in the air waiting for someone with a Pringles can and a PDA and too much time on their hands to come along and surf the web on your dime. There is even a practice called, "War Chalking" in which enterprising folks come along and paint or chalk marks on the walls and sidewalks letting everyone know that you have a wireless network that they think can be cracked and used for all manner of nefarious purposes.

Another scary fact is that unless you happen to catch someone in the act a wireless attack can be impossible to trace. If an attack occurs through the internet it is physically traceable. The router, ISP, and any sniffers that may have been running will have IP information, domain information, logs, and WHOIS data that can usually be tracked back to the attacker or the device that was used. In a wireless penetration the person who perpetrated the attack could potentially leave behind nothing that is traceable to anything physical. One day perhaps we will be issued a wireless ID along with our driver's license and be required to use this for all wireless transactions for accountability. Even then the attackers will be stealing the ID's of innocents and using these to perpetrate their attacks.

In my opinion wireless DOS (Denial of Service) attacks will become part of police and military operations as well as something that Hackers and crackers will use to disrupt day to day activities. All of us have experienced things that cause interference with wireless devices such as cell phones and wireless cards. How long will it be, if they don't exist already, before there is some sort of handheld device that floods the airwaves with interference and shuts down all wireless devices in an area? The long and the short of this is that there are many aspects of wireless security that render it less secure then conventional wired access.

On the other side of this coin wireless does have its place. As you sit at a coffee shop or in the airport if there is a WAP (Wireless Access Point) you can surf the web and get email as you sip your Latté. As long as you are aware that you are public and treat it accordingly there are many excellent uses for wireless. Any place of business that offers public access to the internet can provide wireless without the cost of physically pulling wires. Trade shows and class environments can benefit from the speed and ease of setup.

Created by submitted on 11/10/2003 1:09 PM
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

[27]Having pointed out the actual risks and theorized about other potential problems; if you decide that you want to use wireless at home take the following security steps. Refer to your individual router documentation for exact information on how to accomplish each task.

1. Don't Broadcast your SSID. Many wireless routers broadcast the Security Set Identifier to make connecting easy. This should be turned off to prevent your router from announcing itself to anyone who knows how to listen.

2. Change your Default SSID name. Many routers come out of the box with a default SSID like "Linksys". Even if you aren't broadcasting it there are programs that scan for the default SSID names.
3. Consider a program to flood the Airways with false SSID's. There are programs available that will make it look like there are a host of SSID's in your area. This effectively masks the real SSID and can frustrate those trying to use a WAP without authorization.

4. Filter MAC (Media Access Control) addresses. All network devices have a unique identifier called a MAC address. You can program your Wireless router to only accept connections from know MAC address. This is fairly easy to circumvent, but will still prevent many attacks.

5. Enable and Use WEP with four rotating keys. WEP is a primitive challenge and response protocol that uses a 32 bit CRC check added to the standard packet payload. In layman's terms it is 40 bit encryption. Now day's 40 bit encryption can be broken fairly easily even if you set WEP to rotate the keys.

6. If you choose to use wireless you must be more conscious of monitoring you network and keeping up with MAC addresses as devices are retired or replaced.

Conclusion

When PC security starts to overwhelm you, take it a step at a time and work through each of these security issues in order and you will walk away with a very thorough understanding of your PC security. Maintain these security measures over time and your PC security will stay fit and ready for anything. Remember the old adage, "The Price for Security is Eternal Vigilance." Security will never be done. New patches and exploits come out daily. Security is not something you can do once and then be okay. Keep this document handy and keep up to date with the latest security issues using the bulletins that you subscribed to in the course of this document.

Created by submitted on 11/10/2003 1:09 PM
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References

Cox, P. and T. Sheldon. "The Windows 2000 Security Handbook." Berkeley, CA: Osborne, 2000.

McLean, I. "Windows 2000 Security: Little Black Book". Scottsdale, AZ: Coriolis, 2000.

Schultz, Eugene. "Windows NT/2000 Network Security." Indianapolis: New Riders, 2000.

---

[1] Duke University. "What Are the Guidelines for Choosing a Password?" OIT Security. 25 April 2001. http://www.security.duke.edu/3 (9 September 2003).

[2] McAfee Security. "Virus Characteristics – I Love You." Virus Profile. http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=98617 (9 September 2003).

[3] Virus Bulletin. "VB 100% Award." August 2003. http://www.virusbtn.com/vb100/archives/products.xml?table (9 September 2003).

[4] Microsoft.com. "Automatic Updates." June 2002. http://www.microsoft.com/windows2000/downloads/recommended/susclient/default.asp (9 September 2003).

[5] Microsoft.com. "Windows Update." 2003. http://v4.windowsupdate.microsoft.com/en/default.asp (10 September 2003).

[6] Microsoft.com. "Microsoft Security Notification Service." 10 October 2003. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/notify.asp (10 September 2003).

[7] SANS.org. "Computer Security Newsletters and Digests." 2003. http://www.sans.org/newsletters (10 November 2003)

[8] Zone Labs. "Zone Labs Download." Smarter Security. 2003 http://www.zonelabs.com/store/content/company/products/znalm/freeDownload.jsp?lid=zadb_zadown (10 September 2003).

[9] Microsoft.com. "Microsoft Baseline Security Analyzer." 2003. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/mbsaqa.asp (10 September 2003).

[10] Duke University "Creating an Account Lockout Policy." Securing The Personal Computer. 2002. http://security.duke.edu/securepc/acctlockout.html (10 September 2003).

[11] Duke University. "Disabling the IIS Web Server." OIT Security. 16 April 2001. http://security.duke.edu/windows/disable_iis.html (9 September 2003).

[12] Finnamore, Joe. "Null Session in NT/200." Ver 2.0 December 2001. http://rr.sans.org/win/null.php (20 October, 2003).

[13] Berkley Lab. "Hidden Shares." Operating Systems Windows Security. http://www.lbl.gov/ITSD/Security/systems/windows.html#hidden (20 October 2003).

[14] Paul Asadoorian, "NetBIOS Null Sessions: The Good, the Bad, and the Ugly". Brown University CIRT, Rev 1.1 January 3, 2003 http://www.brown.edu/Facilities/CIS/CIRT/help/netbiosnull.html#_Toc25025304 (20 October 2003)

[15] Duke University. "Creating a User Account." Securing the personal Computer. http://security.duke.edu/securepc/useracct.html (20 October 2003).

[16] Gibson, Steve. "Denial of Service." XP Raw Socket Controversy. 6 October, 2003. http://grc.com/dos/xpsummary.htm (20 October 2003).

[17] Gibson, Steve. "Making Windows XP More Secure." 6 October, 2003. http://grc.com/dos/sockettome.htm (20 October 2003).

[18] Microsoft.com. "Enable and Apply Security Auditing in Windows 2000." Ver. 2.0 3 June 2003. http://support.microsoft.com/default.aspx?scid=kb;en-us;300549#2 (10 September 2003).

[19] The Center for Internet Security. "CIS Security Scoring and Benchmark tools." 2002. http://www.cisecurity.org (20 October 2003).

Created by submitted on 11/10/2003 1:09 PM

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

[20] The Center for Internet Security. "CIS Members." 2002. http://www.cisecurity.org/members.html (20 October 2003).

[21] Microsoft.com. "Best Practice for the Encrypting File System." Ver 4.0. 8 October, 2003 http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q223/3/16.ASP&NoWebContent=1 (21 October 2003)

[22] Microsoft.com. "Improve Desktop Security." Tools & Checklist. 2003. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/ChkList/dsktpSec.asp (10 September 2003).

[23] Dart, Andrew. "Deleted Files Can be Recovered." 19 April 2003. http://www.akdart.com/priv9.html (10 November 2003).

[24] Grant, Thompson. "Is It Really Gone? (A Look at Data Deletion)." http://www.giac.org/practical/gsec/Grant_Thompson_GSEC.pdf (10 November 2003).

[25] CyberScrub.com. "Erase Delete Wipe Overwrite your Sensitive DATA with CyberScrub." 2003. http://www.cyberscrub.com (10 November 2003).

[26] GCN.com. "Just Between You, Me and the Hackers on that Wireless Network." Vol. 22 No. 22. 11 August 2003. http://www.gcn.com/22_22/mobile-wireless/23065-1.html (10 November 2003).

[27] Breeden, John II. "Perils of unplugging: 11 steps to successful wireless security." Vol. 22 No. 30 13 October 2003 http://www.gcn.com/22_30/news/23832-1.html (10 November 2003).

© SANS Institute 2003, Author retains full rights.

Created by submitted on 11/10/2003 1:09 PM
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.