# *Hardening Windows NT*

**Aelphaeis Mangarae [Chris Morganti]**

**[IRC.EFnet.Org #d-u]**

**December 14th 2005**


**http://www.SecurZone.org**

**Join Aelphaeis Mangarae On IRC:**

**irc.EFnet.org #d-u**

# Table of Contents

# Introduction:

Is Windows secure? Can Windows be secure?
These are two questions which are often asked by many people.
To answer the first question, Windows with its default settings out of the box is by far the most insecure operating system there is (OpenBSD being the most secure.)
One of the reasons Windows is often said to be insecure is because it is attacked the most, this is generally because Windows is targeted more because it is more popular.
Script Kiddies, as well as there botnets are constantly scanning the internet looking for windows machines which are set up poorly and/or do not have the latest security patches.
Can Windows be secured? The answer is yes, Windows can be secured with the right knowledge and tools.
In this day and age computer security is extremely important, often people do not know how to secure there machines and that is why they are being attacked, with the help of this guide you will be able to lock down your windows machine.

# Anti-Virus:

Years ago, Anti-Virus software was rare and not entirely necessary, viruses were no where near as rampant as they are today.
Today viruses are released every hour of the day, their purposes vary from just plain trying to be destructive and costing companies money to being able to steal passwords, credit card numbers and banking details.
Today Anti-Virus software is absolutely essential, even if you're not a home user and you're just running a Windows web server, infection is still possible through the spreading of worms such as Code Red 1 & 2 which targeted IIS web servers.

Choosing the right Anti-Virus software for your needs is essential, different Anti-Virus software offer different types of protection, some Anti-Virus software is just plain out better than others.
When choosing an Anti-Virus software you may wish to look at different characteristics of each piece of software, there is more to most Anti-Virus software than most people think.
When Anti-Virus programs are compared against each other, they are normally compared on things like the following: **Detection Rate, Speed Of Updates, Heuristic Analysis, CPU Usage and Efficiency, Script Blocking, User friendliness** and **Product Vulnerabilities.**

**Detection Rate:**

Detection rate is the percentage of viruses an Anti-Virus program manages to detect, there are currently over 150, 000 viruses, most Anti-Virus's despite what they make out only detect around 100, 000 of these viruses.
It is also important to check out what Anti-Virus vendors define as a virus, some AV vendors may not see a joke program as a virus, most would though.
A trick that is often used by **script kiddies** and sometimes other individuals is to compress the file using a file compressor such as UPack, UPX, FSG, Mew, PECompact. It wasn't that long ago that packers like these made Anti-Virus programs totally useless, in 2002 Anti-Virus vendors such as **Symantec (Norton)** and **Network**

**Associates (McAfee)** were not able to uncompress even UPX packed files.

**Speed Of Updates:**

The speed of updates realised by an Anti-Virus vendor is absolutely essential, when Code Red was released on the Internet it managed to scan the whole internet in about 20 minutes and found virtually every vulnerable computer there was. I myself have experimented with various Anti-Virus solutions, some Anti-Virus programs such as **Symantec's Norton Anti-Virus** seemed to have **terrible update times**, sometimes I had to wait 2 or 3 days for an update! I found this to be outright not acceptable and promptly stopped using the software.

**Heuristic Analysis:**

It is most often viruses are detected by **viral signatures** although occasionally, **Heuristic Analysis** manages to identify the file as a potential virus.
What the Anti-Virus program does is check to see what the code inside the file does, if the code inside the file does something suspicious like copy itself to network directories and p2p folders, this would most probably prompt a warning from your Anti-Virus software (assuming it had Heuristic Analysis.)
I mostly find that Heuristic Analysis is almost completely useless and should not be used as a solution at all. Generally speaking people that write malicious code are not going to write a virus that is detected by Heuristic Analysis, although this has actually been the case with a couple of worms such as NetSky and MyDoom where **Panda Anti-Virus** managed to detect the worms using heuristic analysis.

**CPU Usage and Efficiently:**

If you own a large company or even a small one, you want your Anti-Virus program to effectively use the CPU of the computers it is on. If your employees are working on a project you do not want their computer to slow down while they are working, you want the Anti-Virus to work quietly in the background.

I found **Symantec's Norton Anti-Virus** to quite heavily consume RAM and CPU.
**Kaspersky Anti-Virus** used to have a bit of problems with CPU usage (they fixed this in later versions), the amount of CPU or RAM usage has nothing to do with the Detection Rate or the performance of the Heuristic Analysis, but it is something to consider when choosing an Anti-Virus program.

**Script Blocking:**

Some websites (generally malicious) use vulnerabilities in Internet Explorer and other browsers to load **Spyware** and **Viruses** onto a an unsuspecting victims computer.
It is very important that Anti-Virus programs actively scan web pages that are being loaded by a person's browser in order to prevent malicious code from being executed.
Malicious scripts also arrive in the form of email and sometimes exploit vulnerabilities in **Microsoft Outlook**.
I find **Kaspersky Anti-Virus** does an excellent job of this.

**User Friendliness:**

This is fairly simple you don't want an Anti-Virus program that is confusing, you want your employee's to be able to easily delete viruses that are found by the Anti-Virus or better still you may wish for the Anti-Virus to search and find viruses all by itself without disturbing the user of the computer.

**Product Vulnerabilities:**

It isn't often Vulnerabilities are discovered in Anti-Virus programs, but it does happen occasionally, there have been vulnerabilities discovered in **Symantec's Norton Anti-Virus** where scanning of an infected file ends as soon as it starts because of information in the viruses header.
You don't want to use an Anti-Virus program that has Vulnerabilities that can be potentially exploited by a malicious virus or piece of code.

After choosing your Anti-Virus your next step will be to configure your Anti-Virus correctly, you should ensure the following things have been enabled:

*Scanning of all files downloaded over the Internet including through Instant Messaging
*Scanning of all files received in email
*Scanning of scripts viewed via web browser and email
*Start up on windows boot
*Active scanning
*Deletion of any virus infected files found
*Automatic updating of viral signatures and heuristic analysis pattern files

It is essential your chosen Anti-Virus has all of the above features, as they are all essential in trying to prevent viral infection, with out one of them viruses will find away in your machine(s).
There are numerous comparisons that can be found online of Anti-Virus programs, however I recommend **Kaspersky Anti-Virus**. It is well known to be the most superior Anti-Virus.

Below are some links to **Trial Versions** of Anti-Virus software:

**Kaspersky Anti-Virus:**

http://www.kaspersky.com/trials?chapter=154373188

**McAfee Anti-Virus (Network Associates):**

http://download.mcafee.com/us/eval/evaluate2.asp

**Anti-Vir (Freeware):**

http://free-av.com/antivirus/allinonen.html

**AVG Anti-Virus (Grisoft):**
http://www.grisoft.com/doc/38/lng/us/tpl/tpl01?prd=sng

**PC Cillin (Trend Micro):**

http://www.trendmicro.com/download/trial/trial-pcc.asp

**Bit Defender:**

http://www.bitdefender.com/site/Download/browseEvaluationVersion/

**Sophos:**

http://www.sophos.com/products/es/pm/eval/

**NOD32:**

http://nod32.com/download/download.htm

**Norman AV:**

http://www.norman.com/Download/Trial_versions/en

**Panda AV:**

http://www.pandasoftware.com/register.asp?CodigoProducto=13&TipoLead=2&TipoUsuario=1&Tipo=1&Ref=WWEN-TIT5-DES&Idioma=2&Country=US&sec=down

**Dr. Web AV:**

http://solutions.drweb.com/home/demo/

**Avast Home Edition (Freeware):**

http://avast.com/eng/down_home.html

**Sybari:**

http://sybari.com/portal/alias__Rainbow/lang__en-US/tabID__3350/DesktopDefault.aspx

**F-Secure:**

https://www.europe.f-secure.com/download-purchase/download-forms/anti-virus-small-business-suite.shtml

For those of you who don't have Anti-Virus Installed or if you want to test the detection rate of a certain AV, below I will list some Online Anti-Virus scanners.
There is no way should be used as a substitute for a real Anti-Virus solution.

**PC Cillin (Trend Micro):**

http://housecall.trendmicro.com

**Panda AV:**

http://pandasoftware.com/activescan/

**Bit Defender:**
http://www.bitdefender.com/scan8/ie.html

**RAV AV:**

http://www.ravantivirus.com/scan/indexie.php

There are also some websites where you can upload suspected malware for scanning by multiple Anti-Virus programs, these websites include:

http://virustotal.com

http://viruscan.jotti.org

# Password Security:

Password security is definitely an important part of security, normally password security is do with the human factor, it has very little to do with how secure a machine is, it is almost entirely up to the administrator to set strong passwords and password policies.

Here are some things you can do to ensure choosing a strong password:

*Make your password at least 12 characters long, many people have recommended a password of 8 characters long, however due to the fact many people have access to **distributed computing** 8 characters is no where near enough and can quite easily be broken.

*Do not use any words that are in the dictionary

*Do not use the same password that you use for another system, this is most definitely the greatest problem people have with password security, many people use the same password for different purposes.

*Do not think that adding on simple prefixes to your password like "123" will make your password stronger, because they will not significantly make your password stronger.
Often admins add "123" to there passwords in order to make them stronger, the problem is because so many admins make this decision it is very predictable.

*Do not think that converting your password to "leet speak" will increase the security of your password, "leet" versions of words are often added to world lists used for cracking passwords.

*Do not tell other people your password or even hint at it, many breaches companies experience are from within the company itself, you don't want other people knowing your password or having the knowledge to easily guess your password.

*Possibly use **Pass Phrases** instead of Passwords, Pass Phrases are things like a small song lyric, due to the length of Pass Phrases

they are often virtually impossible to crack, they are also easy to remember.

**Ways Passwords Can Be Compromised:**

Sniffed - It is possible to sniff for data travelling across and network and intercept plain text passwords as well as encrypted hashes.

Shoulder Surfing - This is a name given to watching over someone's shoulders while they type there password in attempt to see what they type.

Cracked - If your computer(s) suffer a break in from an attacker he may get access to encrypted passwords and crack the passwords, as mentioned above if you're using standard MD5 encryption and a password below 12 characters it is very easy for an attack to crack the password hash.

Cached Passwords Stolen - Often passwords for many different applications are stored cached on a machine, there are programs publicly available that allow these passwords to be retrieved and converted to plain text, although generally this means the attacker would have to have physical access to the machine.

Guessed - Sometimes people use passwords that are associated with a hobby they have e.g. Video Games, sometimes if a person forgets there password they are given a hint to remember the password (Example being Windows XP), this a lot of the time can be easily guessed.

Given - Sometimes people may openly tell other people there password, it is important that if you have employee's for your company that need privileged user accounts that you make sure they do not give away there password to any other users or potential users.

Stolen From Database - SQL Injection is becoming a big problem with web applications, it is very common for SQL Injection vulnerabilities to be discovered in web applications that keep a database of usernames and passwords.

**The Damage That Can Be Done:**

If an unauthorized user manages to get hold of employee's passwords, even if the user does not have special privileges on the network, they may choose to use there user account in order to start attacking the network anonymously, there are many vulnerabilities in Windows and some other systems that allow escalation of privileges on the local machine as well as the network.
The greatest damage could quite possible be the compromise of your entire network, it doesn't get any worse than this.

**Changing Passwords:**

Passwords that are stored on systems are usually stored as encrypted hashes, important data on a system is usually encrypted (Or at least it should be.)
However if an attacker managers to harvest something like an encrypted hash, the plain text password is not necessarily secure, if an attacker has access to multiple machines that are capable of breaking the encrypted hash, it is very likely it is only a matter of time before the hash is broken.
Therefore it is very important passwords are changed on systems, many security “experts” would probably recommend that passwords be changed every 3 months.
This is not at all sufficient enough, using multiple machines and efficient encryption/hash breaking software an attacker can easily break nearly any password in well under a month, if your password is of sufficient strength an attacker could probably still break it in about a month.
I strongly recommend changing the passwords to all systems and software every month, or more if possible.
There are some guidelines you should go by when changing passwords:

*Follow **ALL** the rules above when choosing a new password
*Do not make the new password similar to the old one
*Do not simply add or take numbers from the end of the old password
*Do not try and generate a new password according to the date the password is created.

*Try to keep the fact the passwords on a system or software(s) have been changed secret, information about passwords should be kept on a need to know basis.

# User Account Security:

User account security is fairly basic.
When an attacker breaches your system, whether it be remotely or locally the thing he wants is access or control the **Administrator** account.
There are some things you should do in order to try and protect the Administrator account from being breached such as:

*Change the name of the Administrator account to something that doesn't seem of much importance such as "Guest"

*Remove the description of the account, this is pretty obvious.
If you change the name of the account yet do not change the description, your efforts are almost pointless.

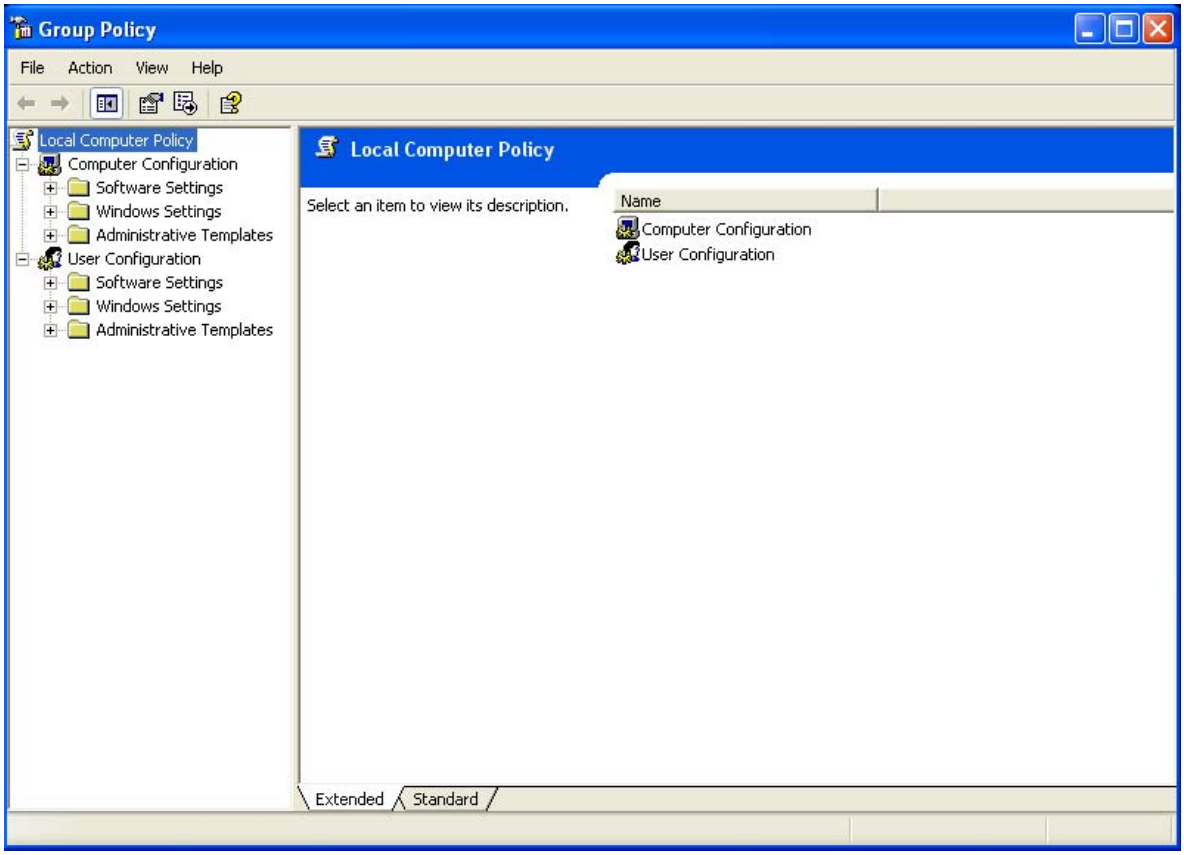
*Give the real Administrator account a very strong password or rather a pass phrase.

*Create a false Administrator account, if an attacker does manage to gain access to this account you would have wasted a significant amount of his time.

*Try to avoid using the Administrator account, if you do not need to use the account simply don't.
If you use an account with lower privileges and it gets comprised, it won't have such a devastating effect on your system/network.

If you find you do not need the Administrator account on your machine you may disable it.

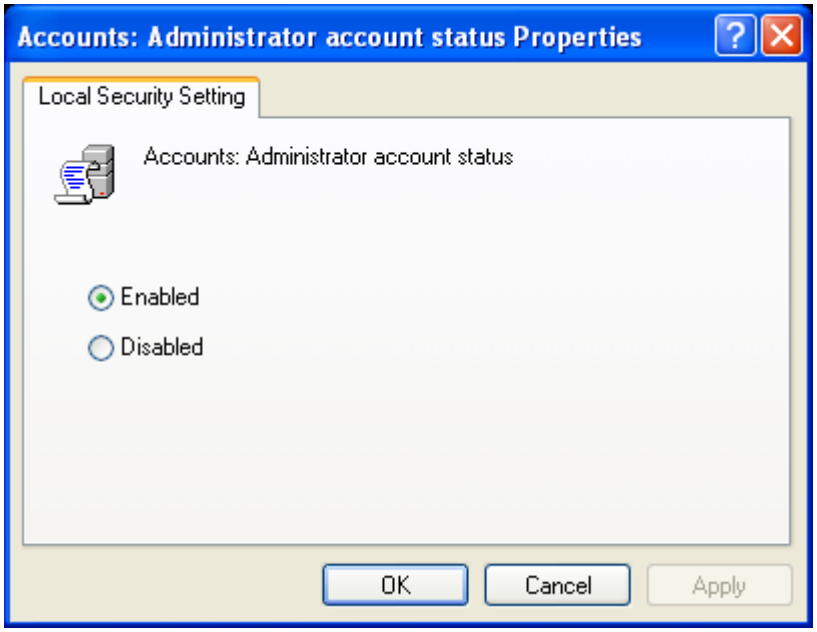
Go to Start – Run then type GPEDIT.msc




**Above is a screenshot of the Group Policy editor.**

If you wish to disable the Administrator account you can go to:

Computer Configuration – Windows Settings – Security Settings – Local Policies – Security Options – Accounts: Administrator account status.



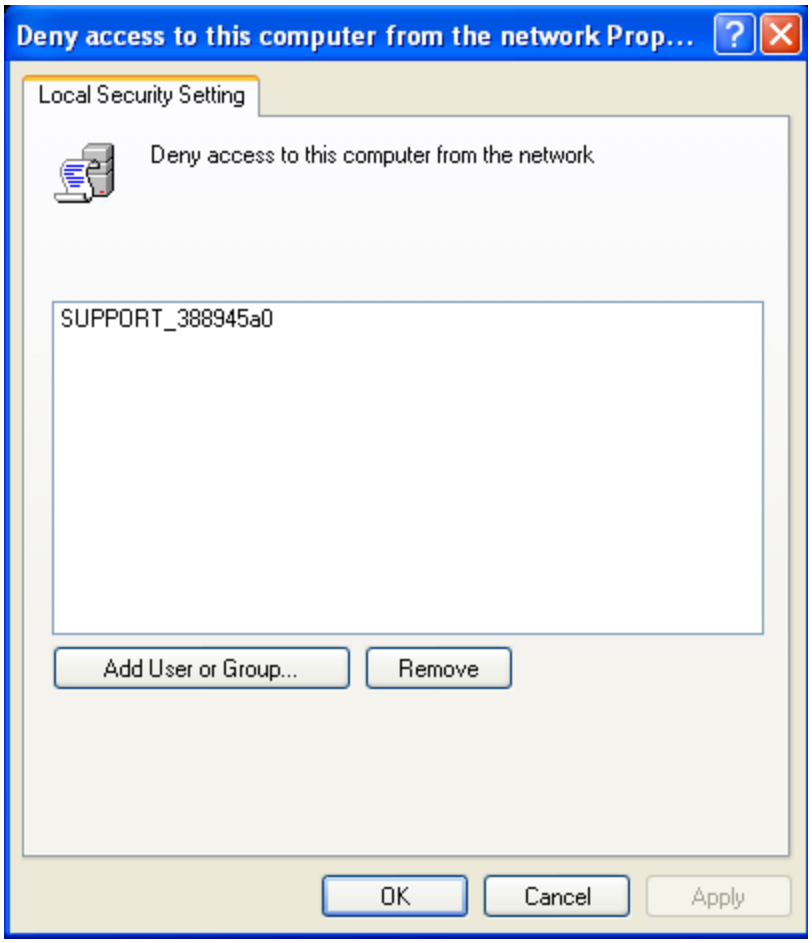

**Above is a screenshot, showing the menu where you can disable the Administrator account.**

If you cannot disable the Administrator account there is something you can do which is quite clever.
You can block access to the Administrator account from the network.

Computer Configuration – Windows Settings – Security Settings – Local Policies – User Rights Assignment – Deny access to this computer from the network.

**Why Is User Account Security Important?:**

If an attacker manages to gain control of an administrator account, he will have the power to do anything on a local machine (That is, if he gains access just locally not on a network level.)
Limited user accounts are of little use to an attacker, once an attacker breaks into a network his goal is nearly always to find a way of elevating his privileges or taking over the Administrator account.




**Above is a screenshot showing the menu where you can disable access to your machine from the network.**

# Spyware/Adware:

Spyware is something virtually every PC user on the face of the earth has been infected with at one point or another, many home users have no Idea there computer is monitoring every action they carry out.
Over all most people are not educated enough about Spyware and are unaware that there computer is monitoring there every action thus causing many problems with there machine.
Many "experts" often see Spyware as a great threat, generally this is a myth, the main purpose of Spyware is to monitor your computers activity for market research.
So generally Spyware is **NOT** a security risk, however since some Spyware may actually store compiled information on a persons hard drive, if there computer was compromised it may be possible for an attacker to harvest this information, or possibly intercept the information as it passes from the victims computer to the owner of the Spyware.
Since Spyware is such a problem which even I have problems with at times, I decided to include details about this in this guide.

**What Is Spyware (In Detail):**

Spyware is software that actively monitors a user's keyboard activity and sends it away to a corporation or person with out the user's knowledge.
In a recent audit done by **Earthlink** over 90 % of computers connected to the Internet are infected with Spyware, Spyware is indeed a severe problem.

**What Is Adware:**

Adware is similar to Spyware and is often labelled as "Spyware". Adware collects information on a user such as there age, location, sex. Buying preferences and Internet surfing habits.
Adware also commonly hijackers users web browsers such as **Internet Explorer.**

The purpose of Adware is collect information on a user in order to display appropriate advertisements to them so the user may be tempted to buy a selected product.
Sometimes corporations that are involved in profiting from Adware often trick unsuspecting users by advertising there products as having no "Spyware", although this is true there product may contain Adware which is actually Spyware, except it is placed into a slightly different group.

**How Are People Infected With Spyware/Adware?:**

People are infected with Spyware/Adware through various means. Huge profits can be made from the use of Spyware or Adware, the most popular method the bad guys use to infect unsuspecting users with Spyware/Adware is to secretly load the software onto there computer via vulnerabilities in there web browser.
There are numerous vulnerabilities in Internet Explorer which allow Spyware/Adware to be loaded onto a victim's computer.
It is common for companies such as **Gator** to use **ActiveX** applets to load the software onto victim's computers.
Microsoft thus disabled ActiveX in there Service Pack 2, which prevents many malicious websites from loading Spyware onto victims computers, however since the release of Service Pack 2, Spyware/Adware companies have found other means of loading there software onto victims computers.
Another method Spyware/Adware companies use in order to install Spyware/Adware on victims computers is to bundle there software with Freeware, when installing software it isn't often users actually read the user agreement to see entirely what they are installing, currently Spyware is perfectly legal.
Many programs such as **KaZaA, Limewire, DivX, eDonkey** and packed with these 3rd party applications.
Beware of Installing freeware, as it may come at the cost of having your computer becoming infected with Spyware, I highly recommend **having a quick read through the user agreement.**

**The Dangerous Of Spyware/Adware:**

The biggest potential danger of Spyware/Adware is the theft of private information, such as usernames and passwords, when this

information is collected and sent away there is no telling who this information is being sent to, or what these people choose to do with this information.
Spyware/Adware often uses a significant amount of bandwidth, users on slow internet connections will most probably be effected greatly by Spyware/Adware streaming away there private information, this has been known to cost people literally thousands of dollars extra in bandwidth costs.
The third danger of Spyware/Adware is damage to your computer, Adware often hijacks your web browser causing severe inconvenience.
Spyware/Adware companies are aware that users will often try and remove there software, and in some cases have specially coded their software to be very hard to remove, some tactics they use include disabling a users **Task Manager** and/or **Registry Editor.**
The greatest potential danger is of course not knowing what the Spyware is doing, Spyware often incorporates stealth techniques, some of these include injecting themselves into other applications in order to bypass firewalls!
Some of the stealth technology in Spyware rivals that of root kits which are available.

**Stopping/Removing Removing Spyware:**

Spyware is not an easy thing to stop, Spyware companies earn huge profits from Spyware/Adware, so they go to almost criminal lengths to increase the amount of computers infected with there **"3rd Party Software" .**
Spyware is most commonly placed on computers through the use of ActiveX or Java Applets, If you are using **Internet Explorer** I would highly recommend you disable both of them and turn your browsers security up as high as it will go with out disturbing your browsing ability.
I also highly recommend **Firefox**, Firefox does not allow the loading of ActiveX applets and has other security measures that also prevent Spyware from being loaded on a person's computer.
The second most popular way Spyware is loaded onto a machine is installation as 3rd party software, when Installing software make sure to look through the user agreement, and remember that just because

the software is labelled as having no **Spyware** it does not mean, it does not have **Adware.**

Even if you are using Firefox, or Internet Explorer with the appropriate security settings the chances are you are still going to be infected with Spyware.
Spyware companies use many other various unknown methods of loading Spyware onto victim's computers, therefore it is necessary to have an Anti-Spyware application to remove these nasty pieces of malicious code.
Some Anti-Spyware software I recommend are **Ad-Aware** and **Spybot:Search And Destroy**.
Beware when choosing an Anti-Spyware application, some of the available Anti-Spyware applications actually come with Spyware, as ridiculous as this sounds it is indeed actually true, this is an example of how sneaky Spyware companies can be.

# Firewall Security:

Many network administrators deploy firewalls on there network in order to try and prevent intrusion.
Each day literally thousands of web servers are breached that are running firewalls.
How can this be? The fact is most administrators do not set up there firewall correctly or do not use strict enough filtering rules.
I am now going to explain briefly what a firewall is exactly, what is can protect you against and how they work.

**What is a Firewall exactly?:**

A firewall is basically a piece of software (or sometimes hardware) that filters traffic over a network or Internet connection in order to attempt to prevent unauthorized access from attackers.

**What can firewalls protect you against?:**

Firewalls cannot guarantee 100 % protection from anything, especially software firewalls.
Buffer Overflows and other vulnerabilities have been discovered in firewalls (although this is generally rare.)
What firewalls can try and protect you against is unauthorized access or really exploitation of a local service by an attacker.
By blocking ports that do not need to access the Internet and filtering access to ports that are allowed through the firewall, a firewall significantly decreases the chance of your machine(s) being compromised.
Firewalls (generally) will not protect you against attacks on web based applications such as forums and login portals, so beware.
Some firewalls such as Zone Alarm Pro try to protect against virus infection, by altering security settings/policies in Internet Explorer and Microsoft Outlook (making it harder for viruses to come through Outlook and Internet Explorer.)

**IP Filtering:**

With certain programs firewalls will restrict Internet access to the program by filtering out IP Addresses that are not part of the network the machine is on.

**Port Filtering:**

Sometimes firewalls detect malicious traffic by checking the remote port of a connection, if the remote port is foreign to the port used by default to that service, the firewall will most probably block it.

**Program Restrictions:**


**Above is a screenshot of Zone Alarms program restriction menu.**

Firewalls also restrict what programs can have access to the Internet and what programs cannot.
This usually stops Trojans and other malware from accessing the Internet.

**Packet Filtering:**

Sometimes firewalls will filter packets that are travelling through certain ports.
For example, a firewall may only allow packets associated with the FTP Protocol to travel through Port 21, if the Firewall sees that shell code is travelling to port 21, the firewall may filter the packets in order to stop an attacker from comprising a machine.

**Freeware Firewalls:**

Zone Alarm Personal Firewall:

http://zonealarm.com

Sygate Personal Firewall:

http://sygate.com

Agnitum Outpost Personal Firewall:

http://www.agnitum.com/

**Commercial Firewalls:**

Armor2net Personal Firewall:

http://www.armor2net.com/

McAfee Person Firewall Plus:

http://mcafee.com

Norton Personal Firewall:

http://symantec.com

# Software Security:

In this section of this text, I am going to give you some tips on using secure software and how to set up software for optimum security.

When using software make sure to:

*Always have the latest version of a piece of software, vulnerabilities are discovered in various software everyday.

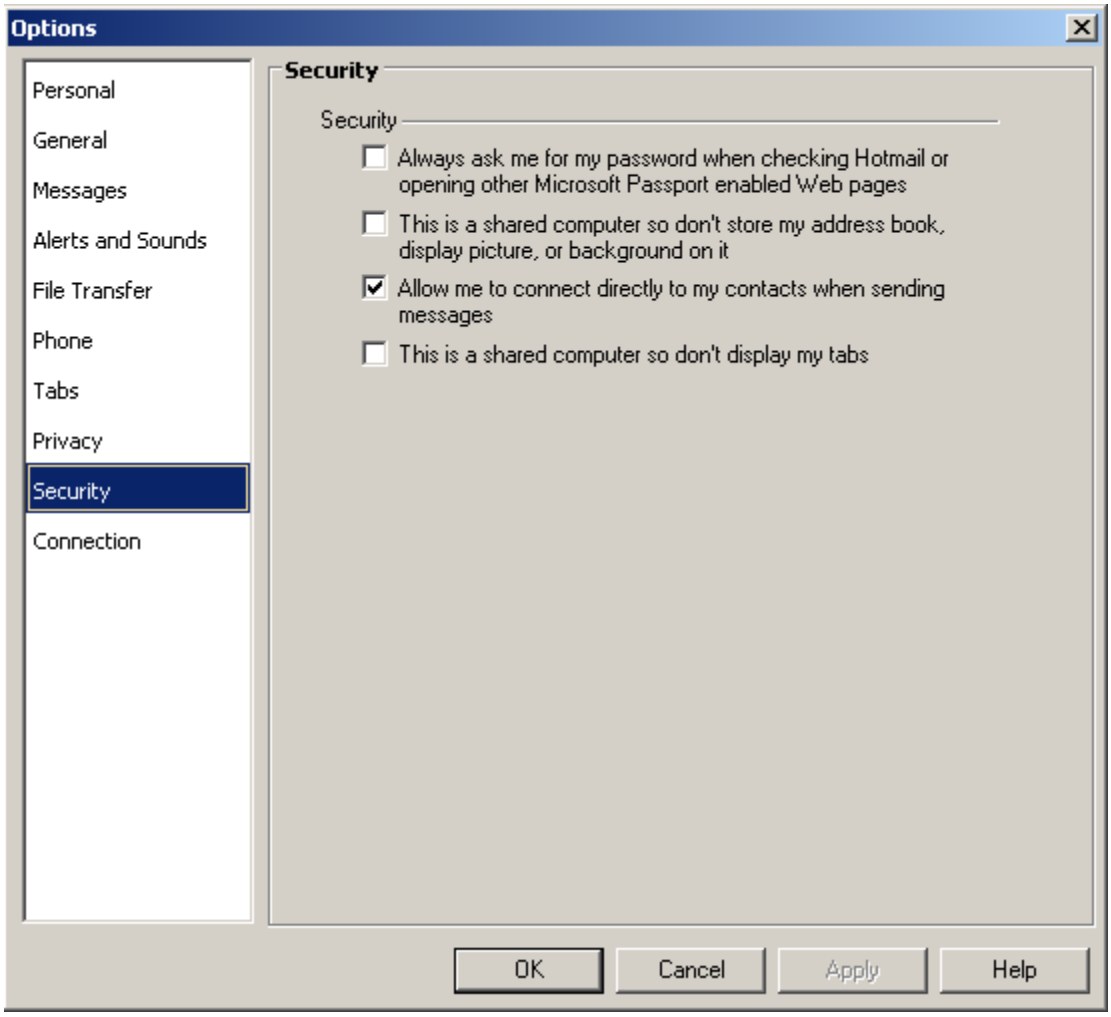
*When choosing software it would be best to choose unpopular software rather than popular, hackers always look to exploit popular software.

*Do not use software which requires updating or patch regularly due to security issues, patches for vulnerabilities are not always released before the exploit. Attackers sooner or later are going to gain access to a 0day exploit for that software.

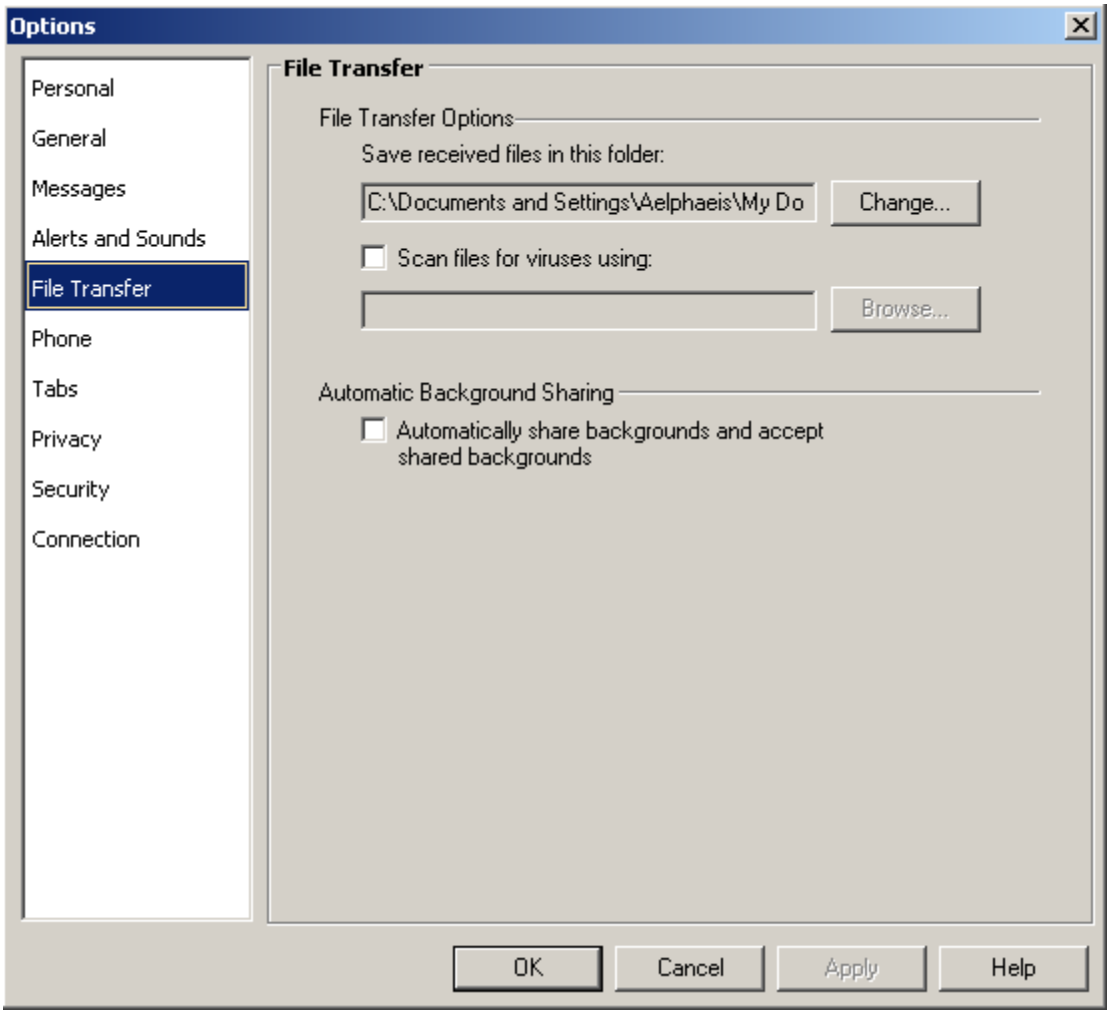
*If possible try to stay away from “Free” software (By “free” software, I mean software that is too good to be just freeware, I am not discouraging you from using freeware at all, there are some very good genuine freeware available, you just have to be careful what “freeware” you use.) Much of freeware software contains Spyware/Adware. If you are looking for a piece of software, I would advise looking on http://download.com
Download.com has a **Zero Tolerance** for software with Spyware/Adware.

**MSN Messenger (IM Client):**

MSN Messenger is a very popular Instant messaging client, the chances are you have it installed on your computer.
MSN Messenger is a very easy program to secure.



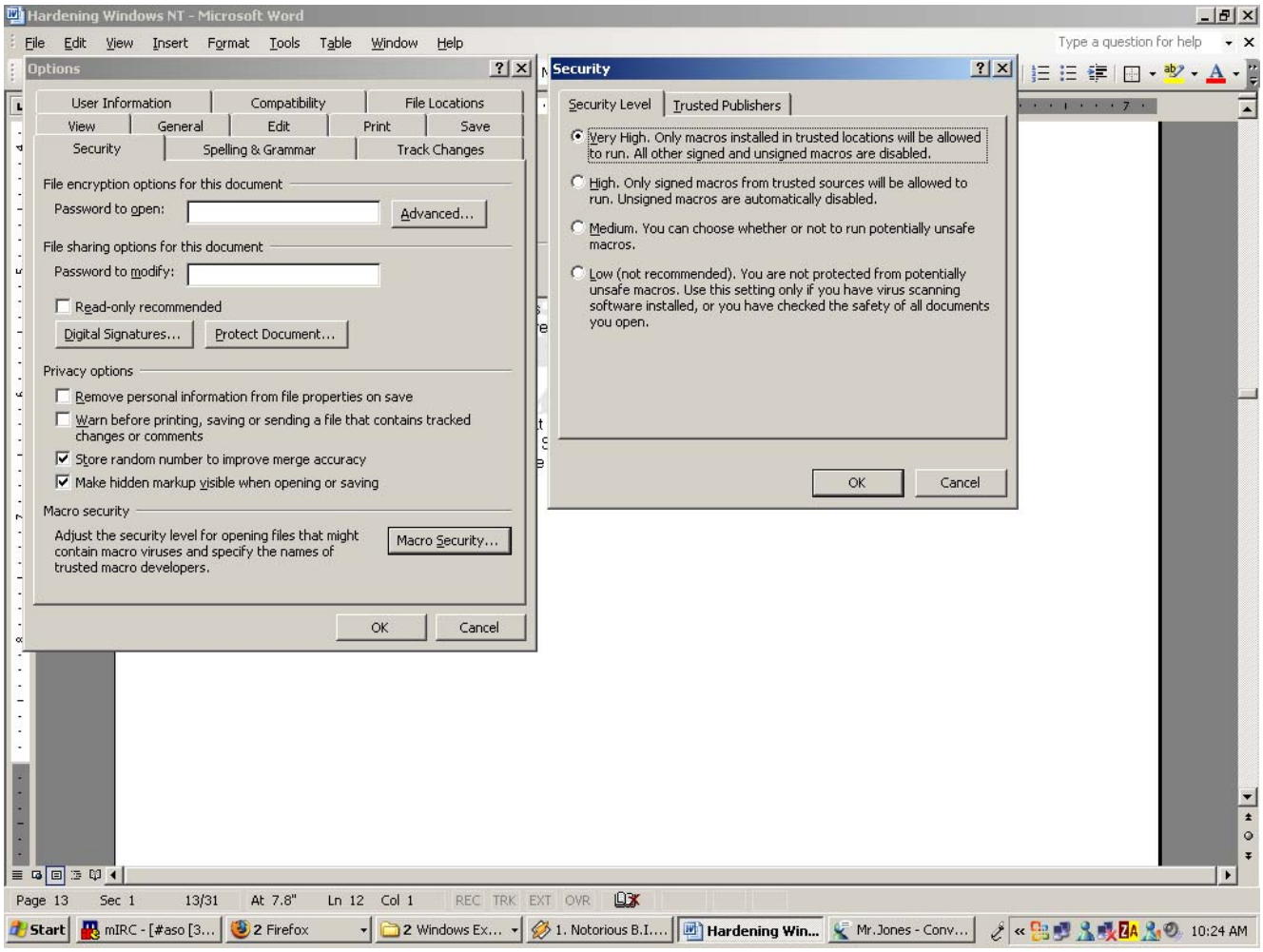

For optimum security I would recommend checking all of the above check boxes.
This should make it harder for someone who has physical access to your computer to cause more damage.




I would personally recommend virus scanning of all received files, even though the latest version of MSN Messenger does not allow receiving of executable files, executable files in compressed archives can still be a threat.

## Microsoft Word (Word Processing):

One of the main security threats that may be present from Microsoft Word is malicious macros.
By default on Windows SP2, Macro Security is set to high, however I recommend turning it up to Very High, you can never have too much security.

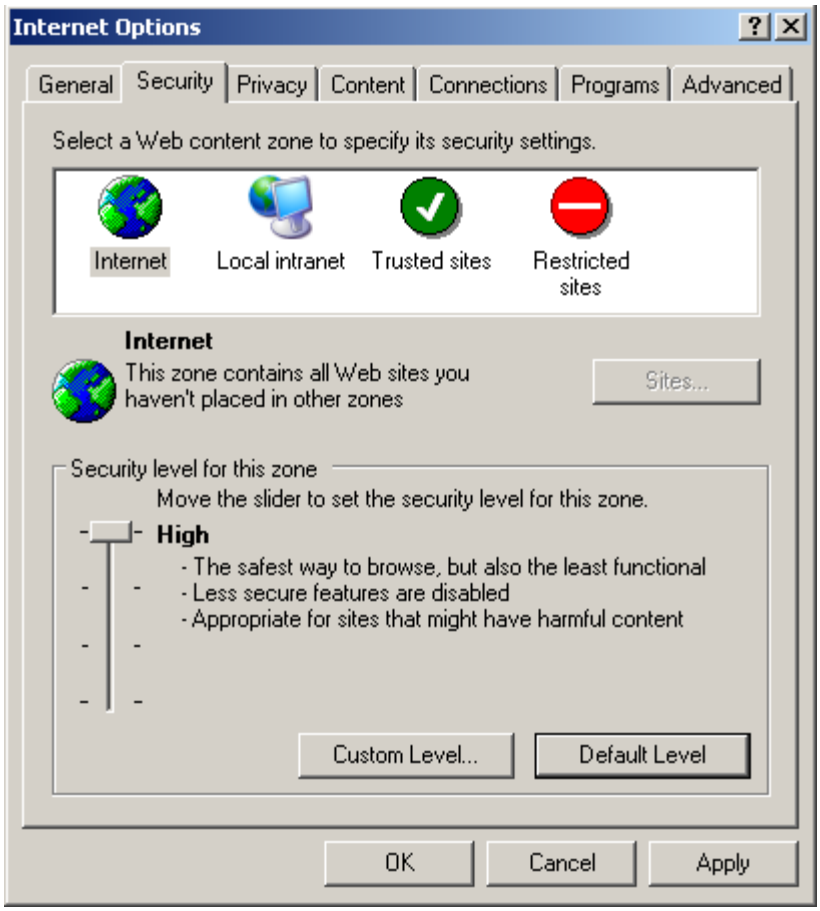



**Above is a screenshot showing where you can turn up Macro Security.**

Apart from malicious macros the only real security risk is Vulnerabilities in Microsoft Word itself, it is of extreme importance you always update all of your software, every time a vulnerability is discovered.

**Internet Explorer (Web Browser):**

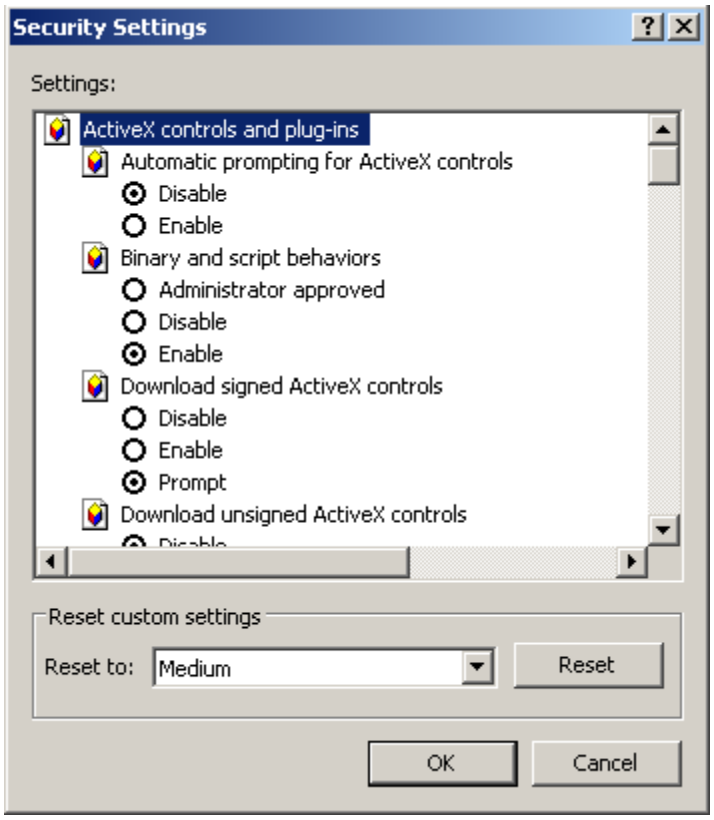
Internet Explorer SP2 out of the box is quite a lot more secure than IE SP1, the reason being that ActiveX is disable by default (thank god.)
However even with ActiveX disable Spyware companies have found ways to manage to still do “Drive by downloads” so they can Install their Spyware.
Almost every desktop computer that has ever been connected to the Internet has been infected with Spyware.
By default In Internet Explorer SP2, zone security is set to medium, this is not at all secure enough for sites that have put effort into downloading and infecting your computer with Spyware.




**Above is a screenshot showing where you can adjust your Zone Security.**

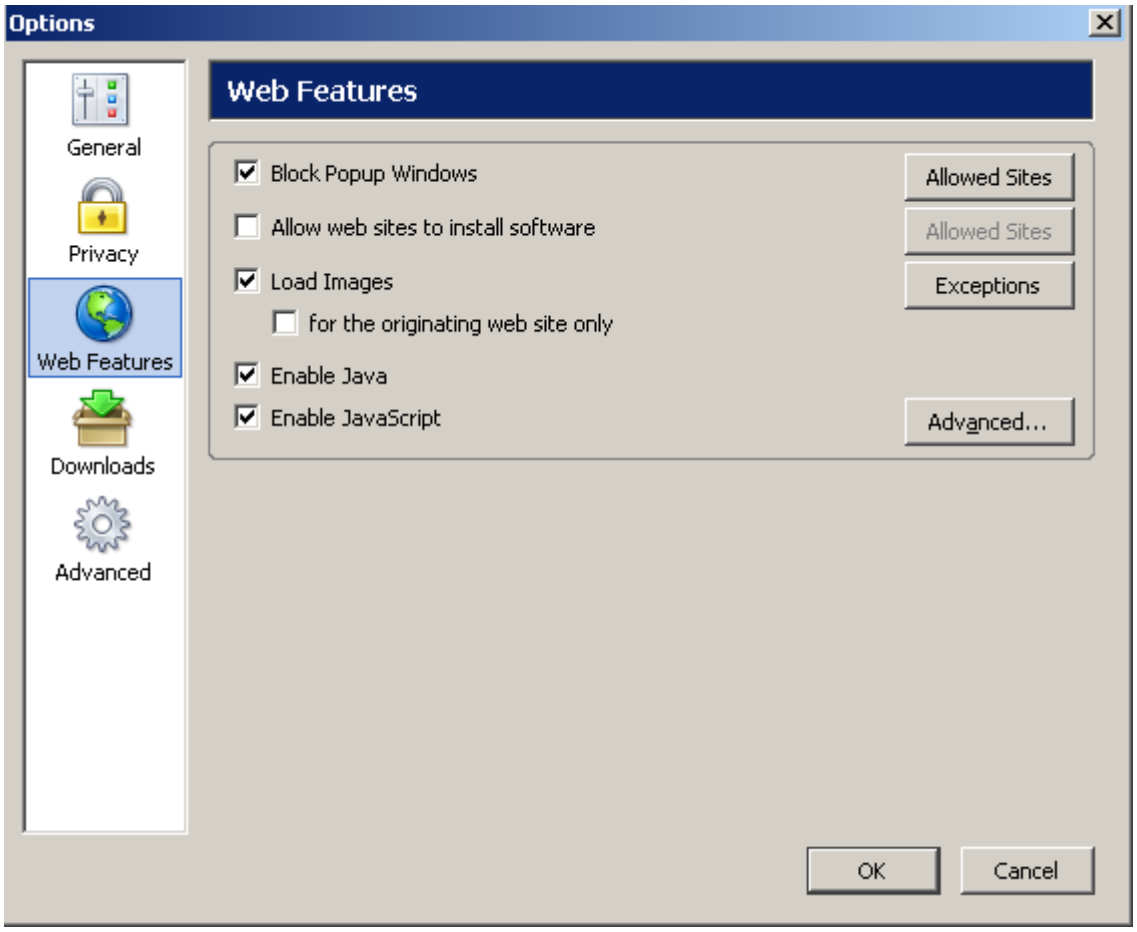
You may find that turning your Zone Security up to High may hurt the functionality of Internet Explorer, however if you find you have no problems with it, I recommend keeping it set on high.

If not you may wish to use a **Custom Level** of security.




**Above is a screenshot showing where you can adjust objects related to security in Internet Explorer**

**Firefox (Web Browser):**




Block Popup Windows:

This is something I strongly recommend you have enabled, for two reasons.
The first being that having popup advertisements display can be extremely annoying at times.
The second is because popup advertisements sometimes download Spyware on to your computer.

Allow web sites to install software:

This is something I strongly recommend you have disabled, it is possible that some rogue groups (Hackers and Spyware companies alike) have found a way of installing software onto your computer with out you being prompted.

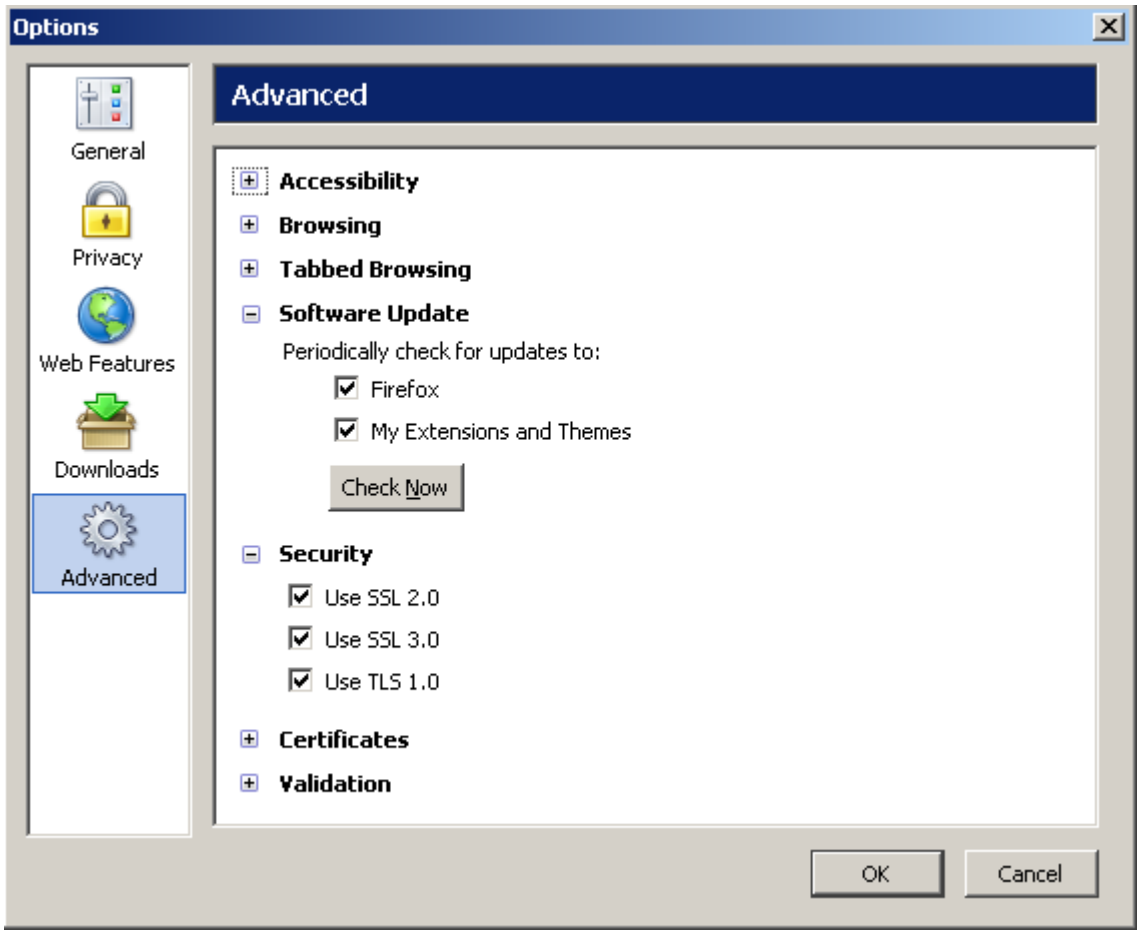
If you are going to install an add-on for Firefox, you should do it manually.

Enable Java:

For optimum security disable Java in your browser, however this will limit functionality in some ways.

Enable JavaScript:

JavaScript is required by a lot of websites, If are you are positively sure you do not need JavaScript disable it.




Software Update:

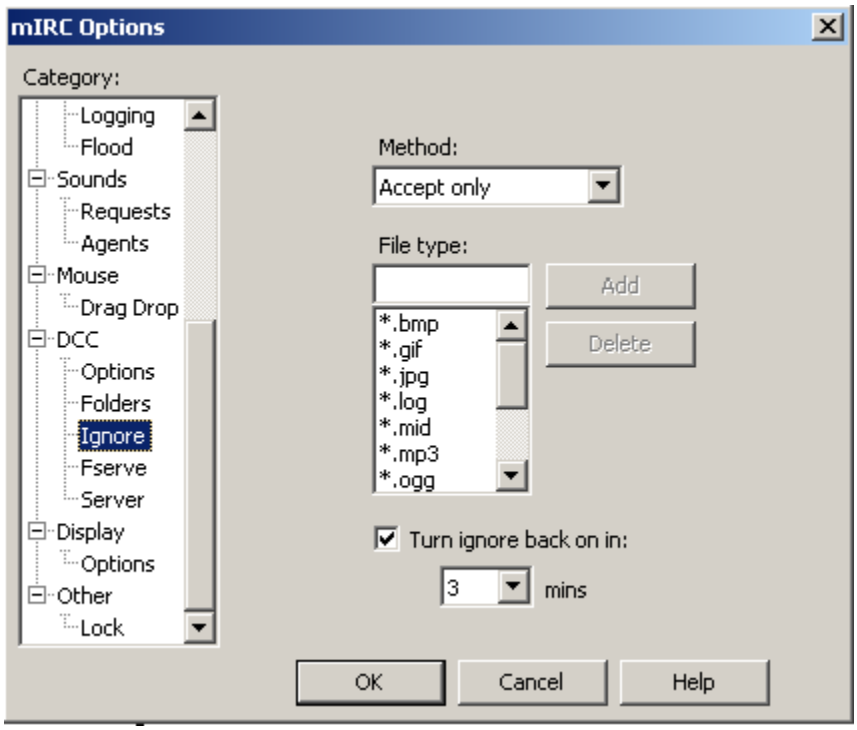
I would strongly recommend that you set Firefox to check for updates for both the Firefox Client and the Extensions and themes.

Security:

If you wish for your data to be encrypted where possible I recommend enabling SSL 2.0, 3.0 as well as TLS 1.0

**mIRC (IRC Client):**

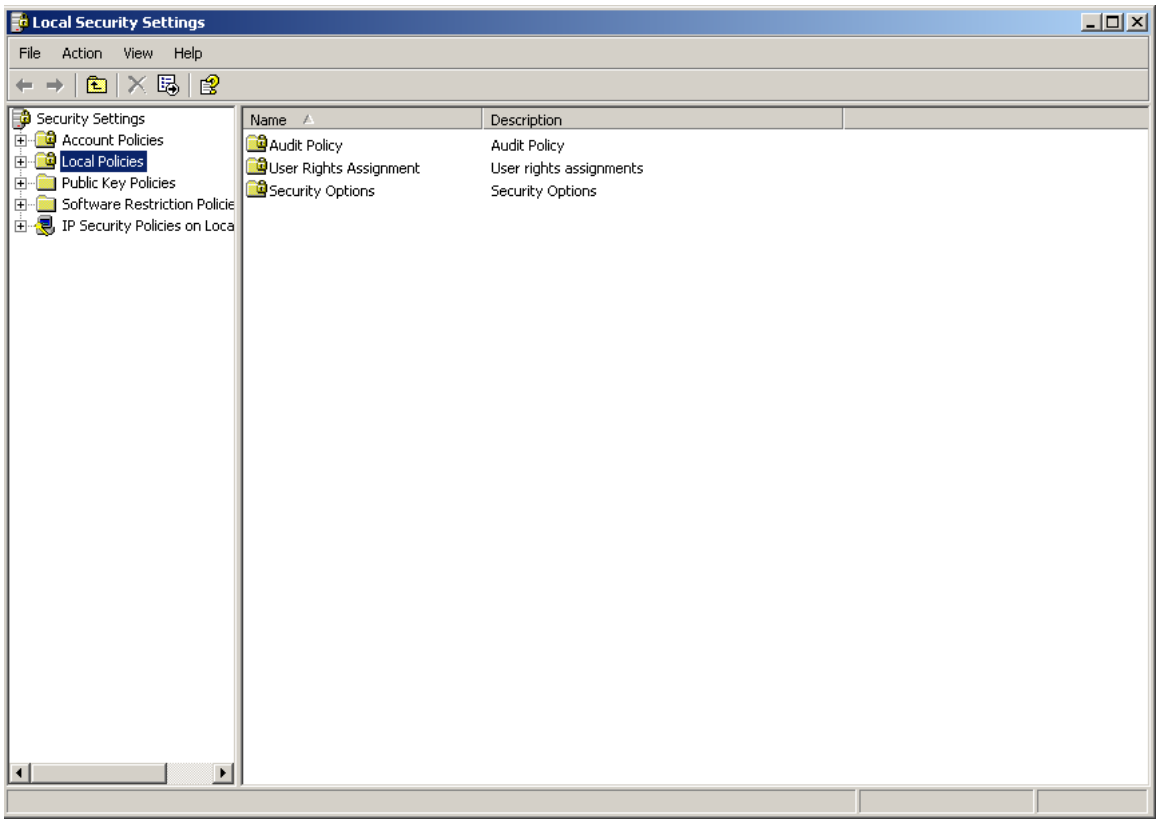
mIRC is quite easy to secure, the only security risk (apart from actual vulnerabilities in the software) is the downloading and execution of malicious files.




You can set it to either allow certain files only, or block certain files. Since there are a range of malicious file types, I recommend using Accept only to filter out malicious files.

# Local Security Policies:

Setting up your local security policies is probably one of the most Important aspects of Hardening Windows NT.




**Above is a screenshot of the Local Policy Editor.**

I am now going to list the password policies and what they should be set to, for optimum security.

### Account Policies – Password Policy

Enforce password history – 0 passwords remembered
Maximum Password age – 30 days
Minimum Password age – 0 days
Minimum Password length – 12 Characters
Password must meet complexity requirements – Disabled
Store password using reversible encryption for all users – Disabled

## Account Policies – Account Lockout Policy

Account Lockout Duration – 15 minutes
Account Lockout Threshold – 3 invalid logon attempts
Reset counter after – 120 minutes

## Local Policies – Audit Policy

We will cover this set of Security Policies in the Auditing section of this text.

## Local Policies – User Rights Assignment

Access to this computer from the network – Administrators, Power Users, Users
Act as part of the operating system –
Add workstations to domain –
Adjust memory quotas for a process – LOCAL SERVICE, NETWORK SERVICE, Administrators
Allow logon through terminal servers –
Back up files and directories – Administrators
Bypass traverse checking –
Change system time – Administrators, Power Users
Create a page file – Administrators
Create a token object –
Create permanent shared objects –
Debug programs – Administrators
Deny access to computer from network – Guest, Student, User
Deny logon as batch job – Guest, Student, User
Deny logon as service - Guest, Student, User
Deny logon locally – Guest, Student, User
Deny logon through terminal services - Guest, Student, User
Enable computer and accounts to be trusted for delegation –
Force shutdown from a remote system – (NONE)
Generate security audits – LOCAL SERVICE
Increase scheduling priority – Administrators
Load and unload device drivers – Administrators
Lock pages in memory –
Log on as batch job –

Logon as service –
Logon locally – Administrators, Power Users, Users
Manage auditing and security log – Administrators
Modify firmware environment values – Administrators
Perform maintenance tasks – Administrators
Profile single process – Administrators, Power Users
Profile system performance – Administrators, Power Users
Remove computer from docking station – Administrators, Power Users
Replace a process level token – LOCAL SERVICE
Restore files and directories – Administrators, Backup Operators
Shutdown the system – Administrators, Power Users, Backup Operators, Users
Synchronise directory service data –
Take ownership of files or other objects - Administrators

**Local Policies – Security Options**

Accounts: Administrator account status – Disabled
Accounts: Guest account status – Disabled
Accounts: Limit local account use of blank passwords to console logon only – Enabled
Accounts: rename Administrator account – Guest12
Accounts: rename Guest account – Administrator
Audit: Audit the access of global system objects – Enabled
Audit: Audit the use of backup and restore privilege – Enabled
Audit: Shutdown system immediately if unable if unable to log security audits – Disabled
DCOM: Machine access Restrictions in Security Descriptor Definition Language – Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor Definition Language – Not Defined
Devices: All undock with out having to logon – Disabled
Devices: Allow to format and eject removal media – Administrators
Devices: Prevent users from Installing printer drives – Enabled
Devices: Restrict CD ROM access to locally logged on users only – Enabled
Devices: Restrict Floppy access to locally logged on users only – Enabled

Devices: Unsigned driver installation behaviour – Do not allow Installation
Domain controller: Allow server operators to schedule tasks – Enabled
Domain controller: LDAP server signing requirements – Not Defined
Domain controller: Refuse machine password changes – Disabled
Domain member: Digitally encrypt or sign secure channel data – Enabled
Domain member: Digitally encrypt secure channel data – Enabled
Domain member:  Digital sign secure channel data (where possible) – Enabled
Domain member: Disable machine account password changes – Disabled
Domain member: Maximum machine account password age – 30 days
Domain member:  Require strong (Windows 2000 or later) session key – Enabled
Interactive Logon: Do not display last username – Enabled
Interactive Logon: Do not require CTRL + ALT + DEL – Disabled
Interactive Logon: Message text for users attempting to logon – Aelphaeis Mangarae 0wnz
Interactive Logon: Message title for users attempting to logon – Digital-Underground.tz4.com
Interactive Logon: Number of previous logons to cache – 0
Interactive Logon: Prompt user to change password before expiration – 7 days before expiration
Interactive Logon: Require domain controller authentication to unlock workstation – Disabled
Interactive Logon: Required smart card – Disabled
Interactive Logon: Smart card removal behaviour – No action
Microsoft network client: Digital sign communications – Disabled
Microsoft network client: Digitally sign communications (if server agrees) - Enabled
Microsoft network client: Send unencrypted SMB passwords to 3rd Party SMB Servers – Disabled
Microsoft network client: Amount of idle time required before suspending session – 30 minutes
Microsoft network client: Digitally sign communications (always) – Disabled

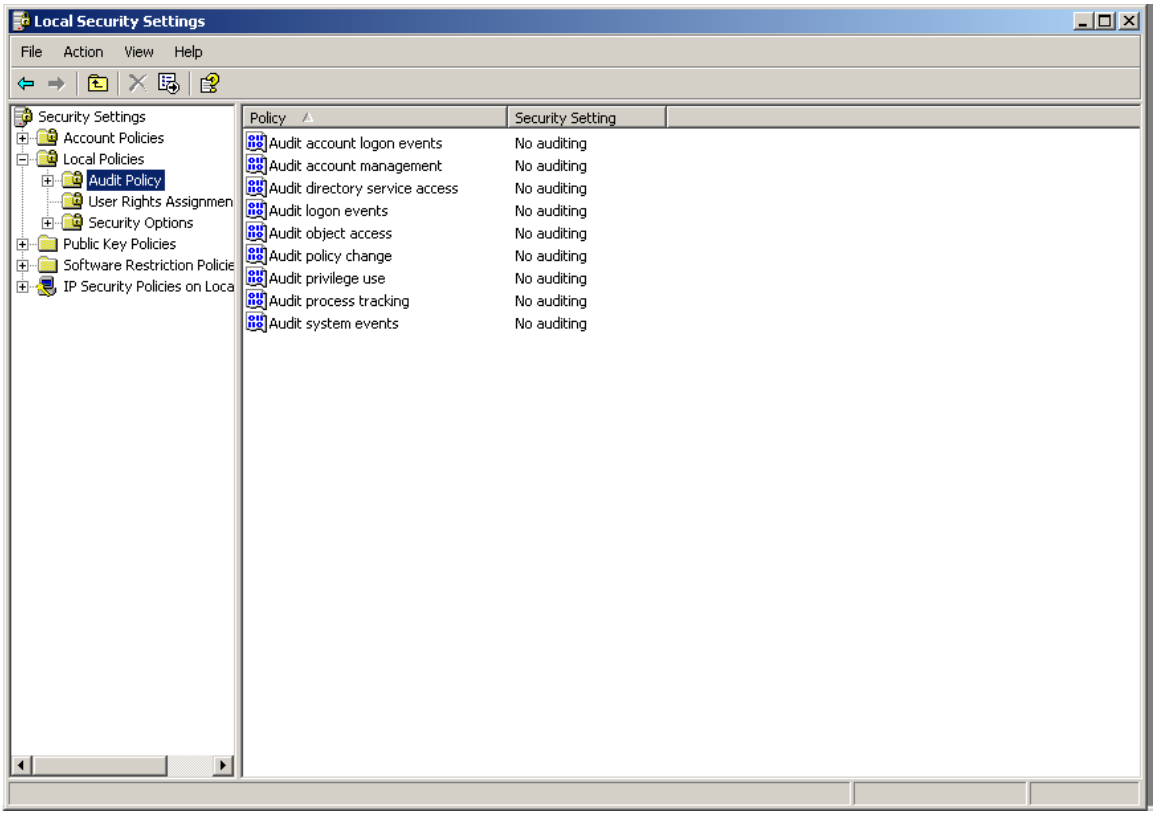
Microsoft network client: Digitally sign communications (if server agrees) – Enabled
Microsoft network client: Disconnect clients when logon hours expire – Enabled
Network Access: Allow anonymous SID/Name translation – Enabled
Network Access: Do not allow anonymous enumeration of SAM accounts – Enabled
Network Access: Do not allow anonymous enumeration of SAM accounts and shares – Enabled
Network Access: Do not allow storage of credential or .NET Passports for network Administration – Enabled
Network Access: Let everyone permissions apply to anonymous users – Disabled
Network Access: Named pipes that can be accessed anonymously – (None)
Network Access: Remotely accessible registry paths – (None)
Network Access: Shares that can be accessed anonymously – (None)
Network Access: Sharing and security model for local accounts – Guest only local users authenticate as guest.
Network Access: Do not store LAN Manager hash value on next password change – Enabled
Network Access: Force log off when log on hours expire – Enabled
Network Access: LAN Manager authentication level – Send LM and NTLM responses
Network Access: LDAP client signing requirements – Negotiate signing
Network Access: Minimum session security for NTLM SSP based (including RPC clients) – No minimum
Network Access: Minimum session security for NTLM SSP based (including RPC servers) – No minimum
Recovery Console: Allow automatic administrative logon – Disabled
Recovery Console: Allow floppy copy and access to all drives and folders – Disabled
Shutdown: Allow system to be shutdown with out having to logon – Disabled
Shutdown: Clear virtual memory paging file – Enabled
System cryptography: Use FIPS compliant algorithms for encryption , hashing and signing – Disabled.

System objects: Default owner for objects created by members of the Administrative group – Object creator
System objects: Require case insensibility for non-Windows subsystems – Enabled
System objects: Strengthen default permissions of internal system objects - Enabled

# Auditing:

After your system has been secured, I recommend auditing the system regularly.
Auditing allows an administrator to see if the security policies and implementations he has applied to his machine or network have worked well.
As part of securing your system you must set your auditing policies up correctly, so when you do an audit you can get the information you want.

**Control Panel – Administrative Tools – Local Security Policy**




**Above is a screenshot of the Local Security Policy menu.**

Unlike other sections of Local Policies there really isn't much to edit.

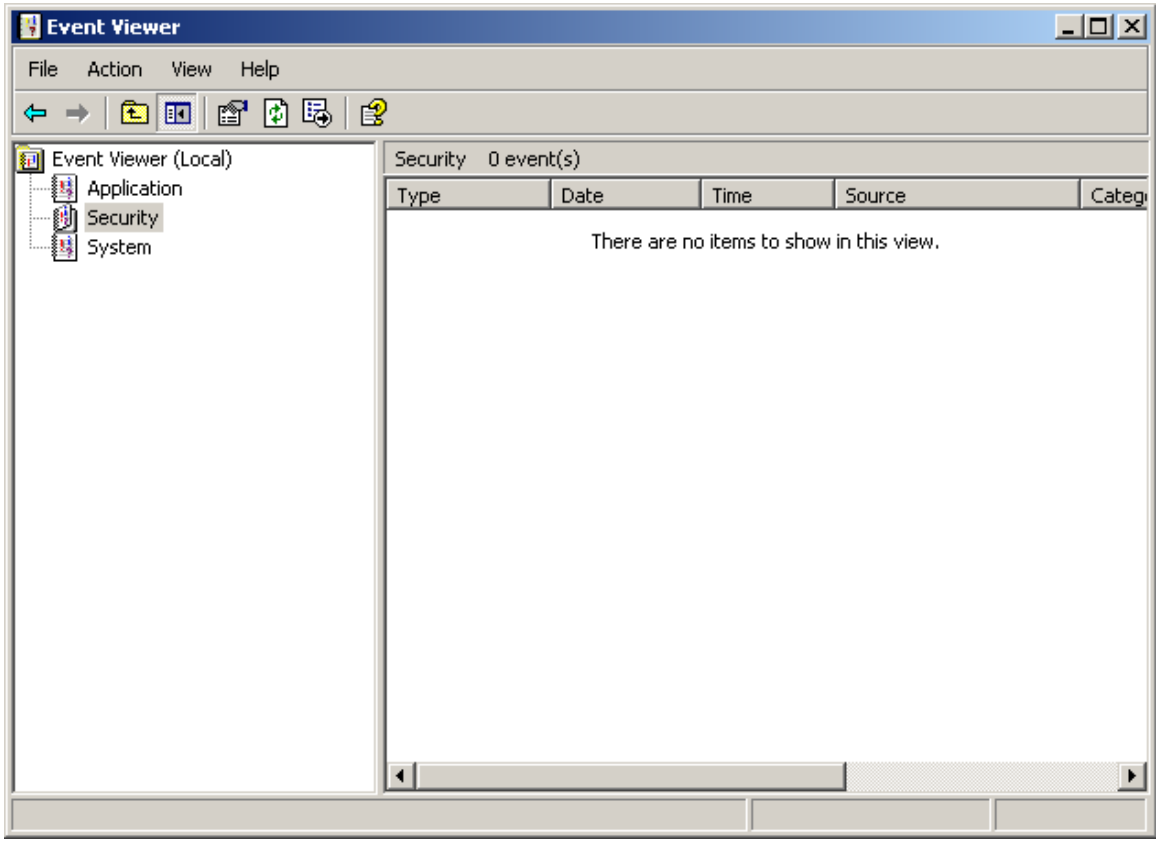
Audit account logon events – Failure
Audit account management – Failure
Audit directory service access – Failure

Audit logon events – Failure
Audit object access – Failure
Audit policy change – Failure & Success
Audit privilege use – Failure & Success
Audit process tracking –
Audit system events – Failure & Success

If you wish you could set both Failure and success for all of them, but this would mean a lot more work on your part as an administrator.

Now that you have set up your security policies for auditing correctly you may wish to view logs on what has happened on your system.

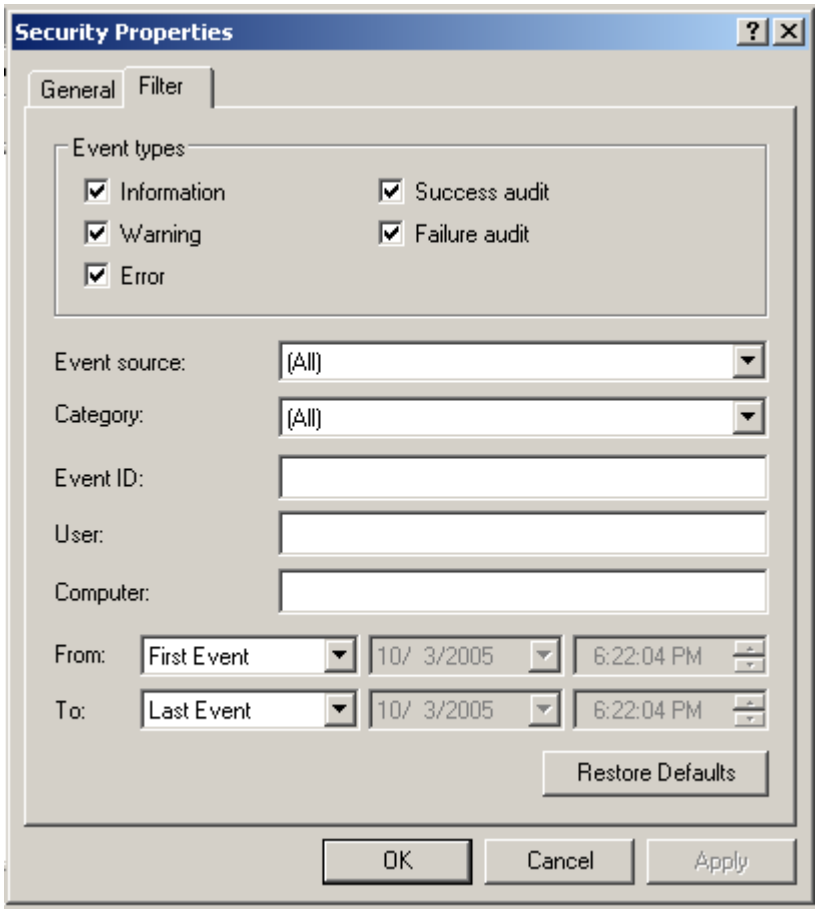
**Control Panel – Administrative Tools – Event Viewer**




**Above is a screenshot of the event viewer.**

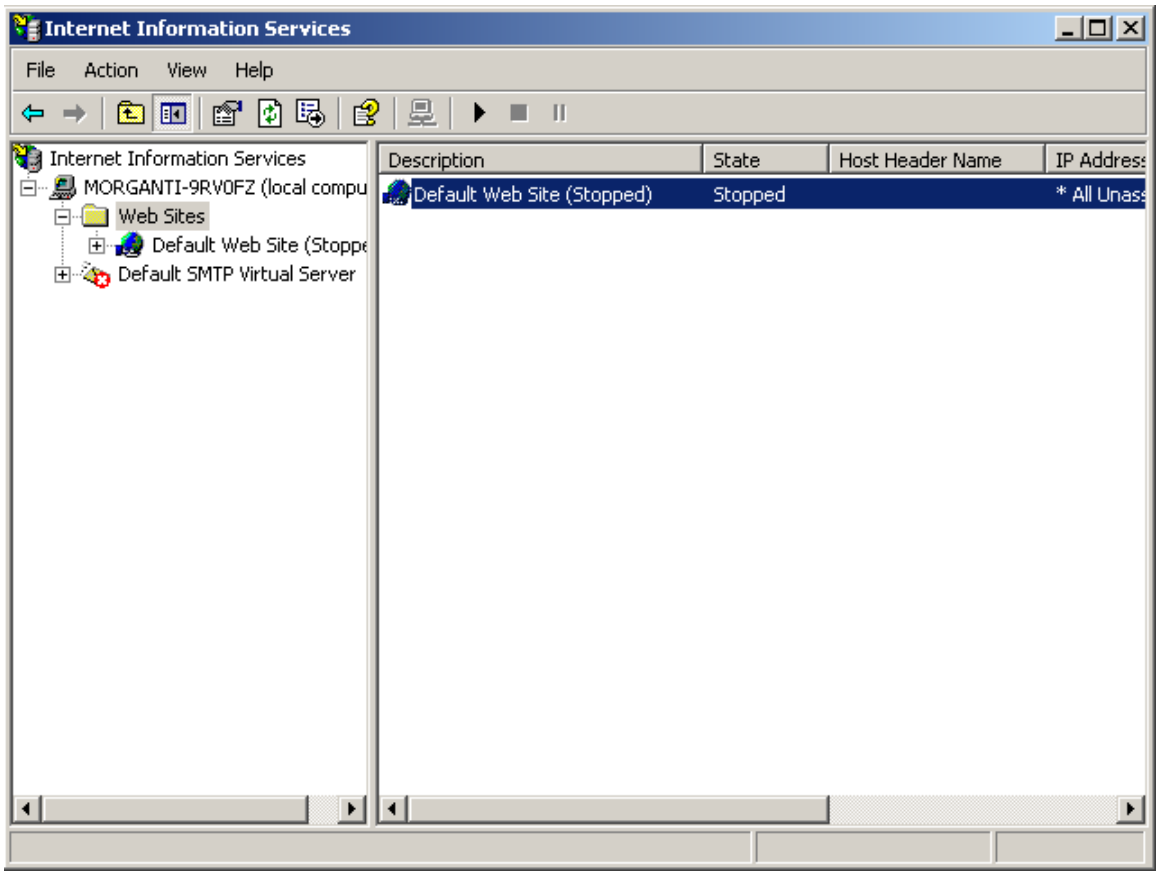
If you have set the local security policy to record both failures and successes of system events, then you may wish to filter the events that are shown in the event viewer.

**Right Click – View – Filter**




**Above is a screenshot of where you can set the filter for the Event log.**

# IIS Hardening (A Brief Look):




Since this text is not focused on securing web servers, I am going to briefly focus on securing IIS (Internet Information Services.)
This part of the text is going to mainly focus on IIS 5.1, the reason being is I at the current moment don't have access to Windows 2003 Server Edition, so I can only Install IIS 5.1 on my Windows XP Pro machine.

If you are running Windows 2000 or 2003 server edition and wish to disable IIS, you can disable the server by going to

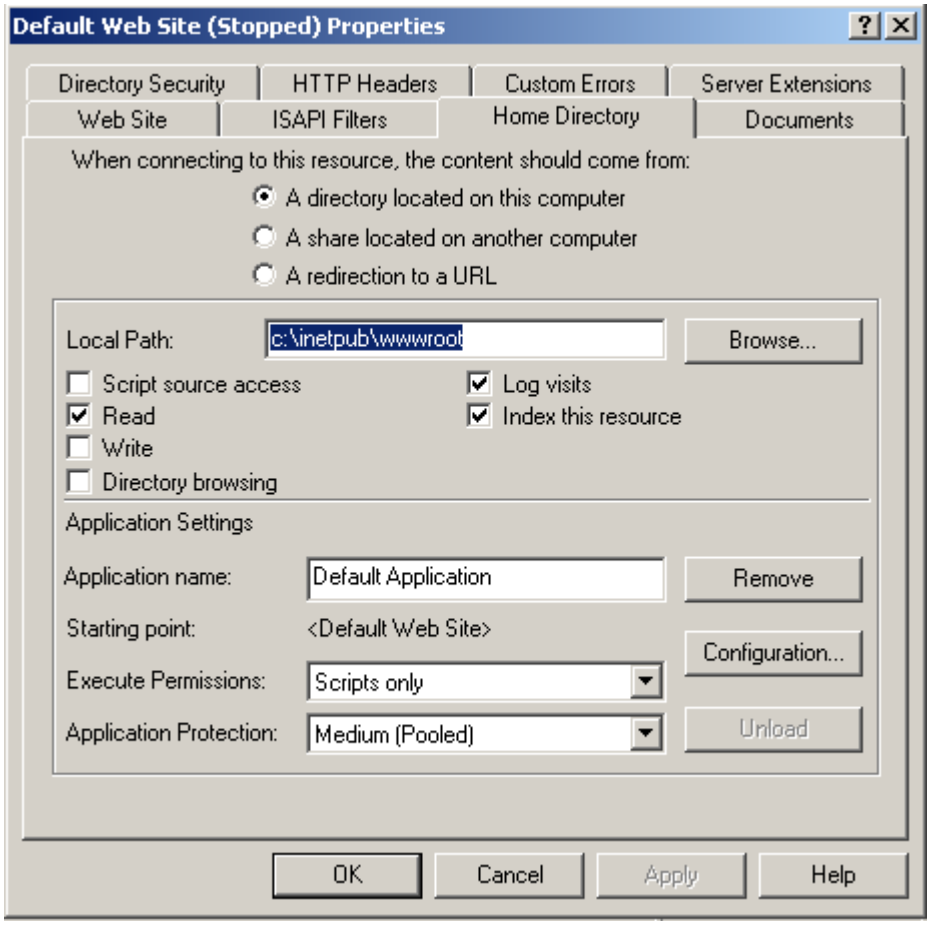
**Run – Services.msc – them Disabling "IIS Admin"**

First of all, and I cannot stress this enough it is extremely important that you keep up to date with all the latest patches.
Make sure you have IIS 6.0 Installed with all of the latest patches.

Recently a website defacing group called **core-project** broke into some military computers, how did they do it you ask? The servers were running IIS 5.0.

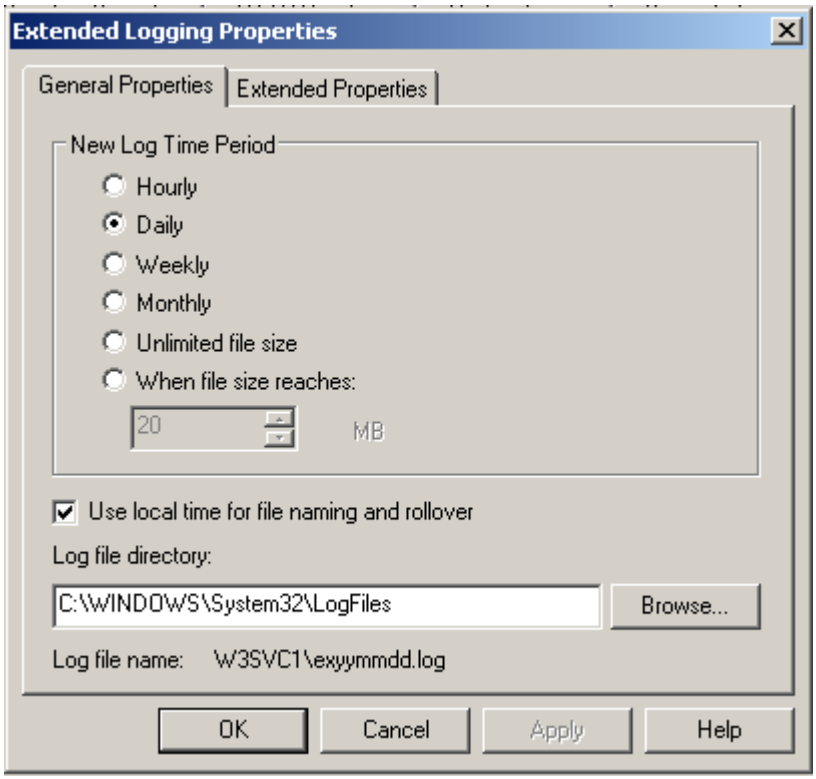
I am now going to list a dozen things you can do to make your IIS server more secure.

1. Change the directory where all of your files are stored.



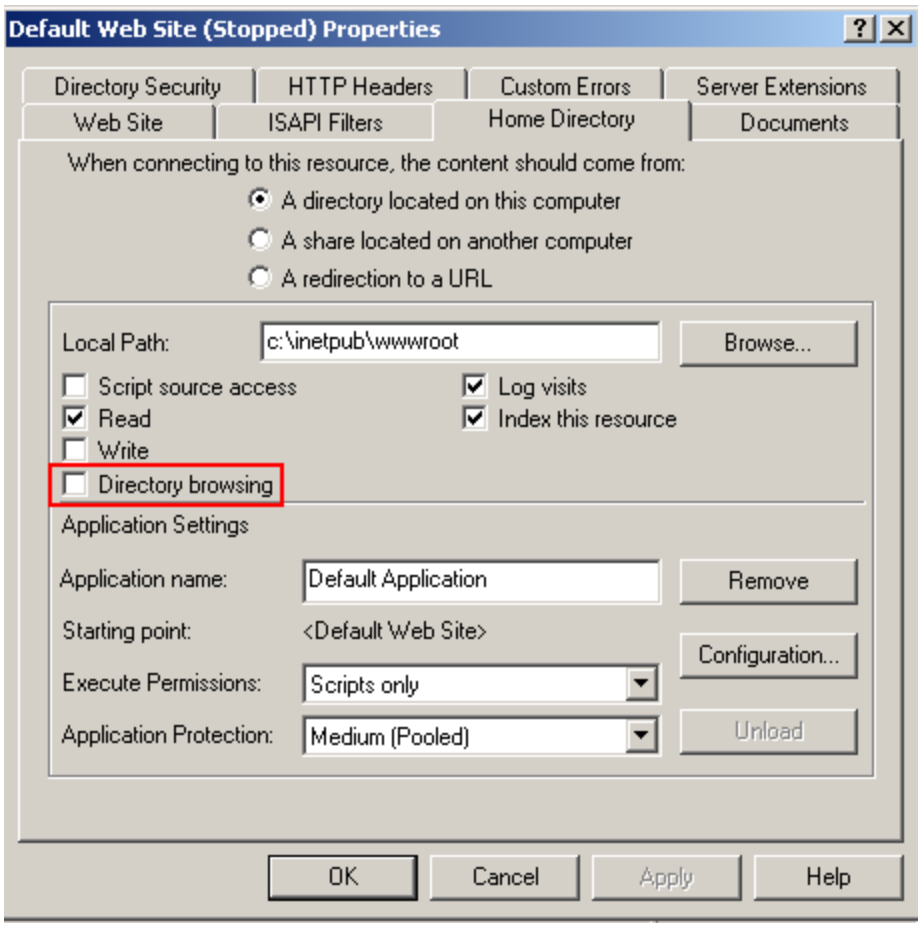

2. As you can see above you can also set whether or not IIS can write files to the root directory, if your website does not contain something like an upload script (something that needs write access), I stongly recommend you check that users only have Read access to the servers.

3. When attackers break in, after they have stolen your information, the first thing they are going to do (most probably) is delete the log files, so there is no trace of them left on the servers.
By default on Windows 2000, the log files are stored at C:\winnt\system32\logfiles\
On Windows XP they are stored at C:\WINDOWS\system32\logfiles\




I think it is extremely important that you change the location of your log files, this should at least help you track down amateur intruders.

4. Turn Directory browsing off, directory browsing will allow an attacker to view all public files, including those that aren't linked to on your website.




**Make sure the box circled in red is NOT ticked.**

5. Set the amount of connections to the web server to unlimited.
Why? There are attack tools available that take advantage of the maximum amount of connections a web server will allow.
Basically what these tools do is make numerous connections from the attacker's machine to the web server.
A script kiddie can easily cripple a web server if he has access to one of these programs.

6. Remove default files that come with IIS, an attacker could use these to positively identify the version of your IIS web server, as well as other sensitive information.

7. NEVER run IIS web server with administrator privileges, if an attacker manages to exploit your web server software, he will have administrator rights on your machine (locally.)

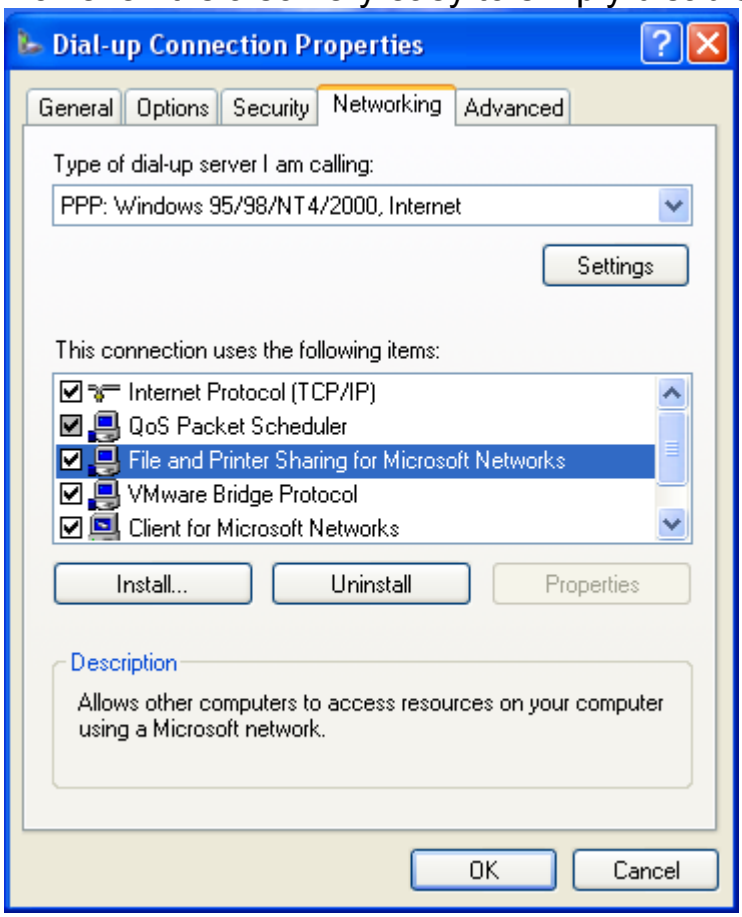
8. This is sort of unrelated, to IIS, but I thought I would mention it anyway.
Once an attacker gains access he will probably utilize some of the software that comes with windows, such as:

Command.com
Cmd.exe
ftp.exe
telnet.exe
tftp.exe
regedit.exe
regedit32.exe

Make sure only Administrators have the privileges to run all of the above.

# NetBIOS/SMB Security:

What is NetBIOS?
NetBIOS is a service on your computer that typically runs at port 139, the purpose of the service is to enabled other computers on a network to view network shares, see other computers connected to the network and use devices such as printers.
The problem with this is that other users on the Internet are also able to view this information, very important information can be compromised very easily by an attacker.
A simple solution to stop attackers could be to block **TCP Port 139** and **TCP Port 445.**
However it is also very easy to simply disable these services.



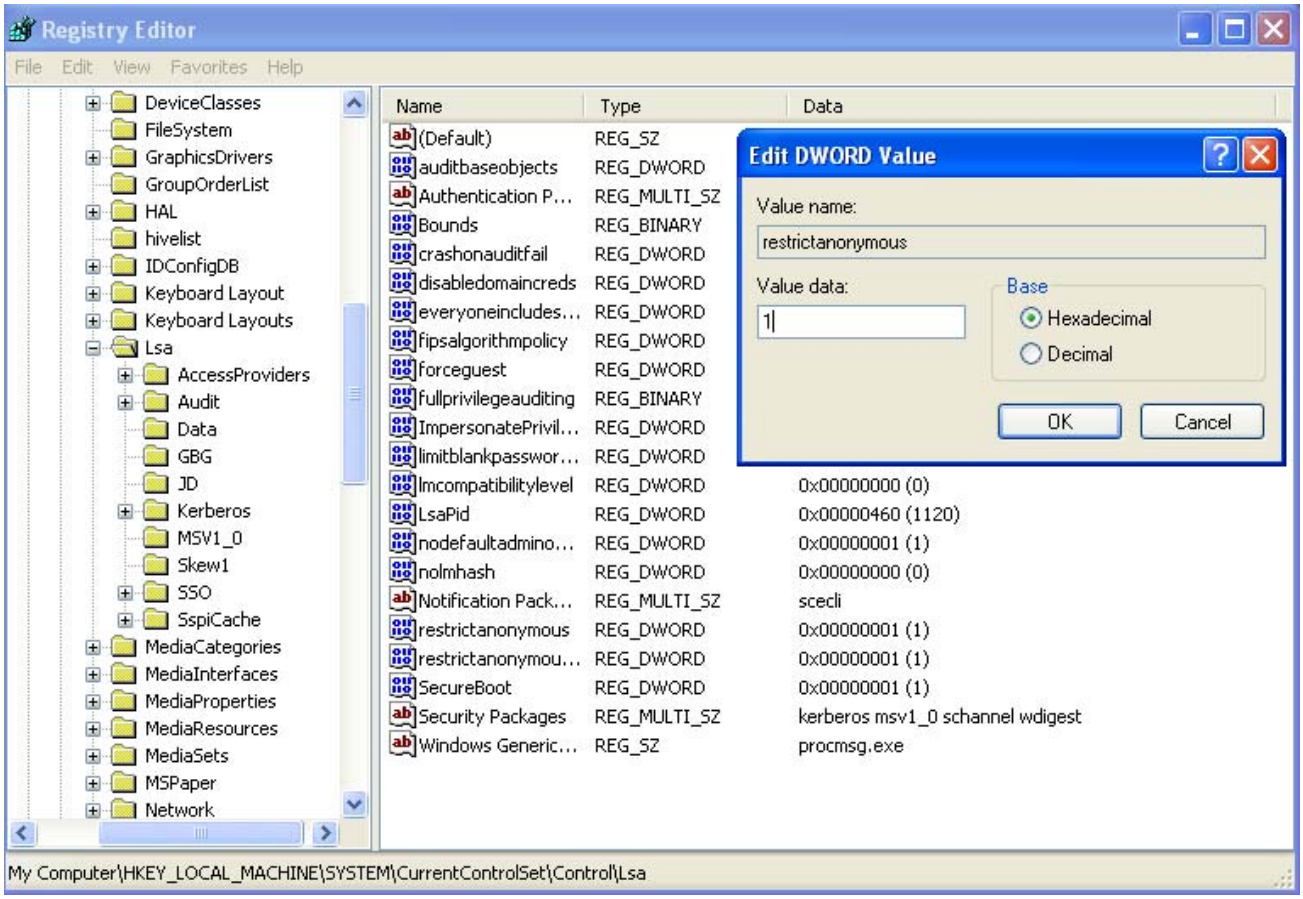

Simply uncheck **File and Printer Sharing** in order to disable the service.
Some problems may arise from disabling the service, these problems may include:

*The ability to be able to operate as a WINS Client may be lost.
*You may not be able to logon to a Windows 2000 domain.
*Some programs that are dependent on accessing information on a network available through SMB or the NetBIOS will not work.

If you do not wish to disable NetBIOS/SMB you can choose to simply restrict anonymous users from logging onto your computer via the server, however the service itself may be a security risk if there were buffer overflows discovered in it.
If you are going to share part of your hard drive, I would strongly recommend using a password that follows the guidelines I have laid out above.
You can restrict anonymous logins by simply editing your registry:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\

Edit "restrictanonymous" and change the value from “1” to “2”, this will make it so anonymous person(s) will be unable to logon to your computer via NetBIOS/SMB.

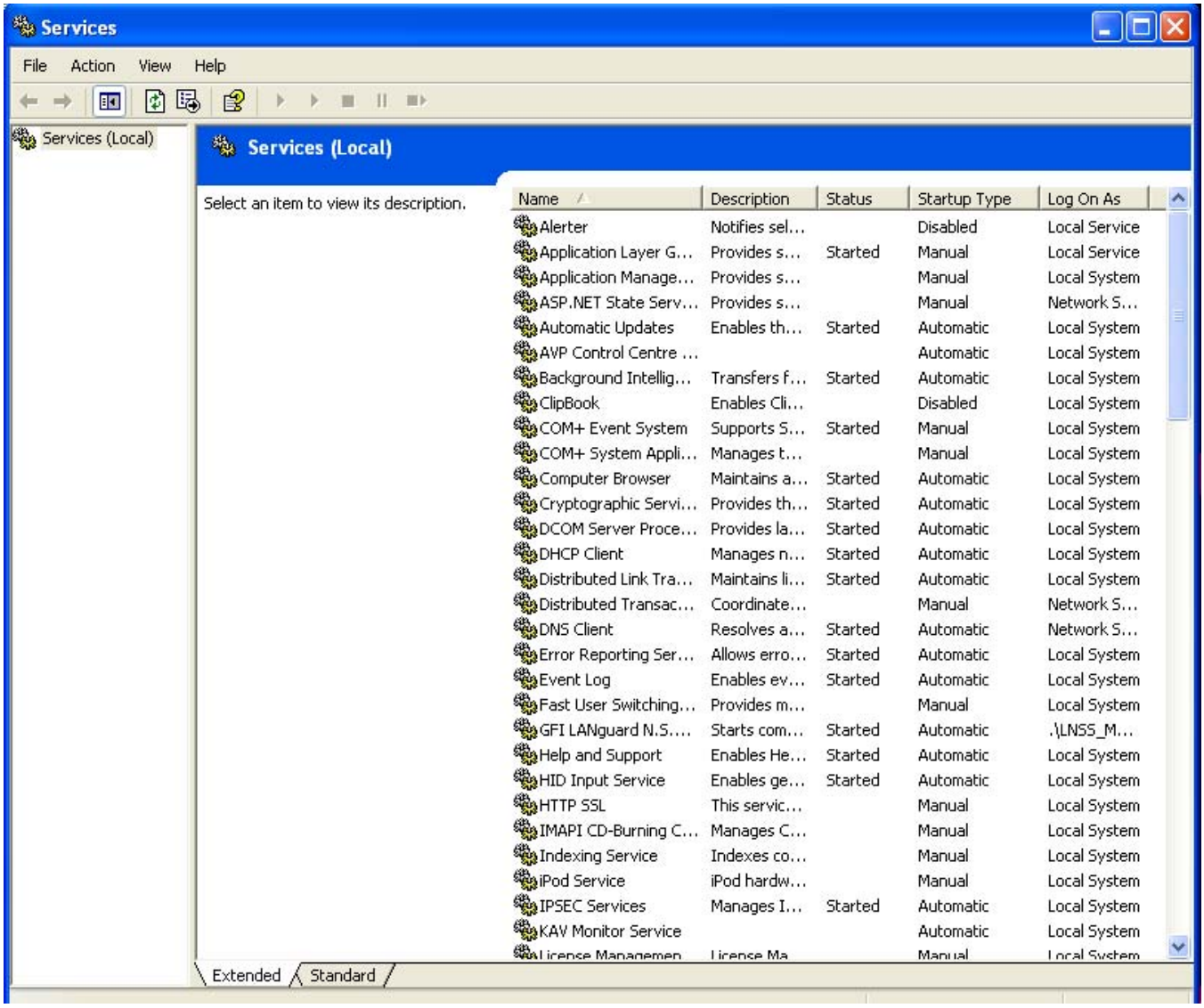



You now need to reboot your system in order for the changes to take effect.

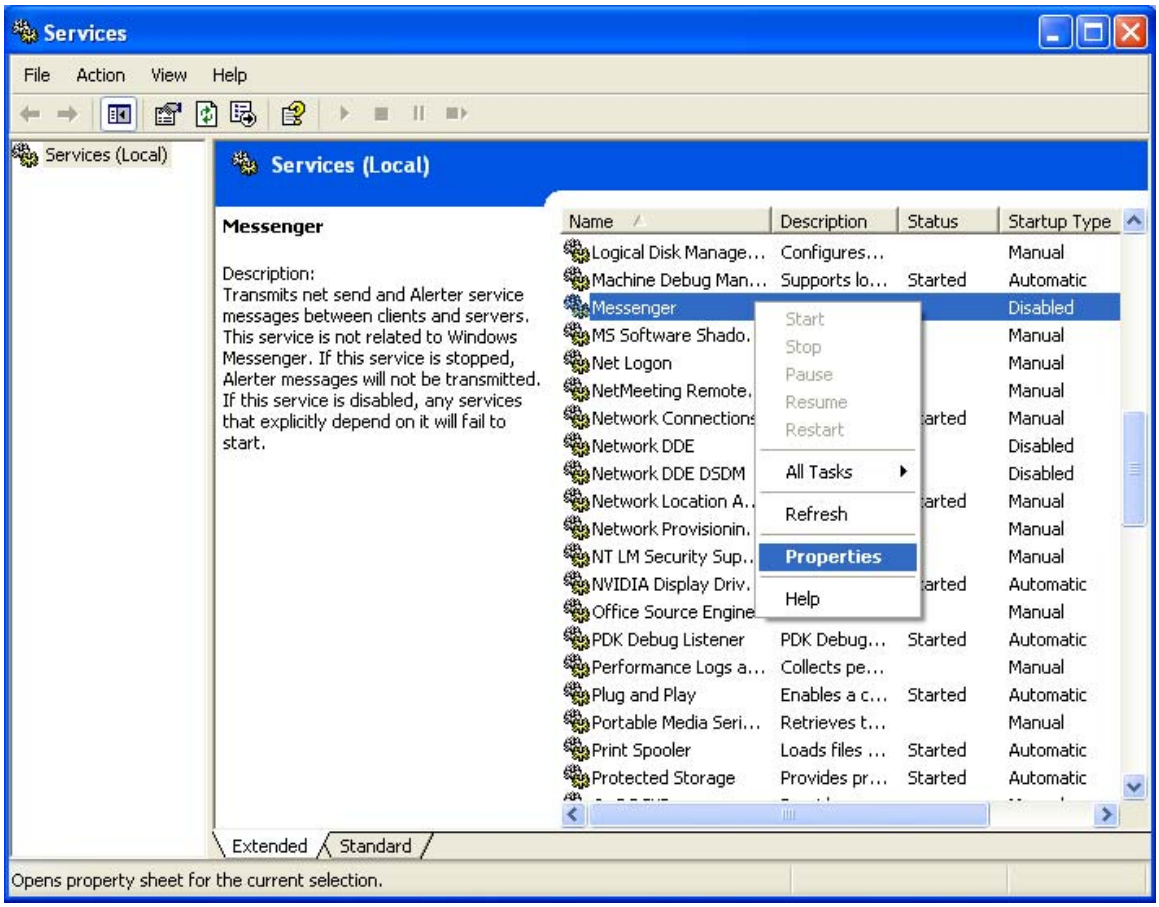
# Services (Security):

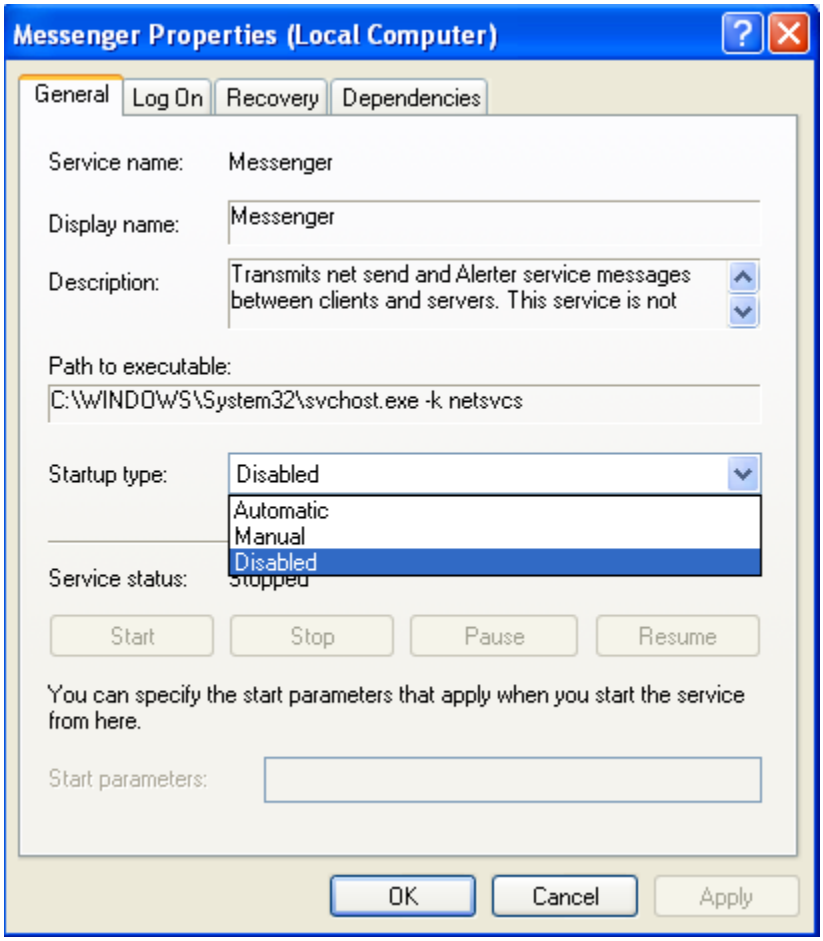
There are many services running in windows, many of these aren't even needed.
The more services that are running, the more services there are for an attacker to exploit, therefore it only makes sense to disable these services to help harden windows.
If you wish to see what services are running in windows:

**Start -> Run -> Type "services.msc"** (with out quotation marks.)



There are quite a few services which you may wish to disable for performance and security reasons.
Below I am going to document unnecessary services and there purposes, but before I do I will explain how to disable a service and how to set a services status to **manual.**
If you set a service to manual, Windows will only start the service when it is requested.






You should now know how to disable services and how to set the properties of some services to manual, now let's finally have a look at different services and there uses.

**Messenger**

Sends messages back and forth from Client to Server, unrelated to MSN Messenger or Windows Messenger.
Disabling this service will also prevent you from getting SPAM windows messages.

**Universal Plug & Play**

UPnP is a set of networking protocols that were made in order so that programs can easily communicate between each other, some File Sharing programs use UPnP.

Generally UPnP is not needed and should be disabled for security reasons, unless this service is required by a certain program that you make use of, please disable this service.

**Remote Registry**

This is a service which allows remote users to be able to connect to your computer and administer your system registry, this obviously should be disabled.

**Automatic Updates**

I recommend leaving this service **enabled**, however If you wish to be in control of the updates for your machine you can disable this, however I strongly recommend to have it enabled, although it isn't necessary.

**Server**

Allows you to share files over your network, I would recommend disabling this.

**Task Scheduler**

I would personally disable this one, it isn't likely any program you use is going to depend on it.
This service could be used by an attacker to elevate there system privileges.

**Terminal Services**

Allows other machines to connect to your machine with remote desktop.
If this is enabled, I strongly recommend disabling this service.

**NetMeeting Remote Desktop Sharing**

Enables a user to connect to your computer with NetMeeting, I strongly recommend disabling this service.

**Secondary Logon**

Allows a user to start a process under different user credentials, you don't want attacks to be able to exploit this, so I recommend disabling it.

**SSDP Discovery Service**

Used to locate UPnP on your network. The chances are you aren't going to use this service so disable it.

Most of the above services should be easily disabled with out causing any harm to your machine, after disabling the services above attacks have a lot let less services to be able to exploit.

# Vulnerabilities (About):

### What is a vulnerability?:

When people talk about software vulnerabilities, they are talking about bugs or errors in the software code that allow a malicious attack to usually remotely cause the software to do something unauthorized.
There are various types of vulnerabilities that are discovered in Windows systems, such as:

### Buffer Overflows:

Buffer Overflows are the result of poor programming, when a programmer codes a program and fails to make the program check what and how much data is being inputted by a user.
For example, a program receives data via a Winsock and stores the data in a memory buffer that is 256 bytes in size, this program however does not check the size of the data sent and just places the received data into the buffer. What if someone was to code a program or rather an **exploit** to send an unusual amount of data? When the data is sent and placed into the buffer, the buffer would overflow causing places in memory to be overwritten.
With out going into detail about the subject (because this isn't the purpose of this text) the attacker could cause specially crafted code to be executed in memory (which is obviously a bad thing.)

### DoS (Denial of Service):

As with buffer overflows, programmers do not always make there programs check what data is being inputted, inputting the wrong type of data or too much data can cause programs to crash or possibly use a great amount of CPU or RAM, this can be for various reasons depending on how the program was made.

### Weak Encryption:

Many programs often store custom data in files, this data can sometimes contain sensitive information such as usernames and

passwords, it is often programs such as FTP Programs store this information encrypted, so the password cannot simply be gathered by an attacker.
However, because data is stored for the purpose of being later retrieved and used, it is not impossible for an attacker once he has the encrypted information to decrypt it himself.
Some programs have problems with using encryption that is not strong enough, and therefore a way of decrypting it is discovered and made public and software is coded by hackers that allow people to easily convert passwords from there encrypted state to clear text.

**Privilege Escalation:**

This type of vulnerability can be present for many reasons, Privilege Escalation is when an attacker uses a **exploit** in order to elevate his or her Privilege on an Operating system or a piece of software.
This could take place, if an attacker was able to get a program running with administrator privileges to execute another program (that program would then be running with the same privileges.)

**What Is An Exploit?:**

An exploit is a piece of code, or a program that is able to leverage a vulnerability in a piece of software to allow something to occur which an attacker could use for his or her advantage.
As far as exploits for Windows vulnerabilities goes, the exploits are normally coded in C, this code is distributed publicly on the Internet and it is very easy for anyone to get a hold of it.
The most common type of vulnerability that is exploited in windows is the buffer overflow, because it usually allows the attacker to gain a remote shell (access to command prompt.)
Here is an example of a publicly available exploit that will grant an attacker a shell on a vulnerable system:
http://www.frsirt.com/exploits/20050812.HOD-ms05039-pnp-expl.c.php

**Patches/Updates:**

After (generally) an exploit is released, the vendor manages to patch the vulnerability and a patch of upgrade is made for the software.

The patch generally follows the exploit, it is only sometimes that a patch is released before an exploit is.
Generally a hacker will notify the vendor of the vulnerability just before he releases the exploit on the Internet, some hackers are very nice and allow the vendor to patch the vulnerability before the exploit code is released, however this rarely happens.
It is **extremely** important that you always have the latest patches and updates applied to your windows machine, as soon as they are released they need to be downloaded and installed.
There are sometimes myths whether or not these patches work or not, most of the time these are myths, most of the time the vendor is able to patch the vulnerability which sometimes is just an error in one of the lines of code.

**0Day Exploits:**

A 0day exploit, is an exploit for vulnerability in a piece of software where no patch exists (usually the vendor doesn't know about the vulnerability.)
0day exploits are not publicly available and are kept private by hackers, they are often used by black hats to penetrate corporate and government systems, since there is no patch for the vulnerability (which most of the time isn't even known to exist.) There is generally no way of stopping an attacker from using a 0day exploit. Therefore it is strongly recommended to have a **firewall** and other forms of protection to stop 0day exploits from being effective (or at least try.)

# Service Pack 2:

Service Pack 2 was released in August of 2005, since then and even before it was released, there has been many articles written about SP2.
Some IT Security Experts have said, Service Pack 2 does a good job of hardening Windows, others have complained that SP2 has not done enough or even worse that SP2 has even caused problems with there operating system. I decided to do a section about Service Pack 2, to explain what it is, what it does and the good and bad things about it.

I will first start off by detailing the many improvements and features that have been incorporated into Service Pack 2.

**Buffer Overflow Protection:**

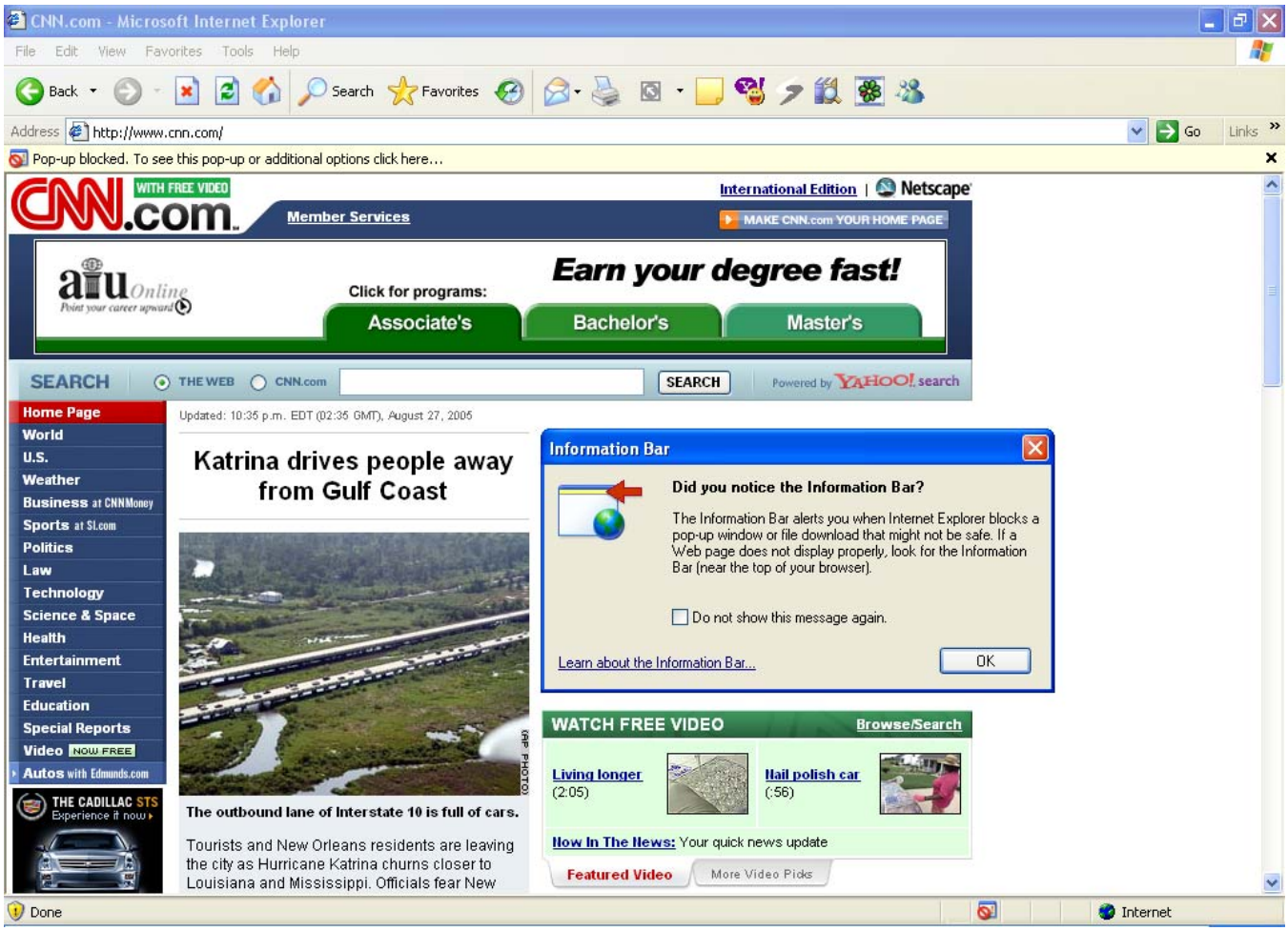
Before the release of Service Pack 2, the main security issue in Windows XP was the Buffer Overflow (I have explained in this text what a Buffer Overflow is.)
In Service Pack 2 Microsoft found a way of preventing both Stack and Heap overflows.
The Buffer Overflow protection works by placing “cookies” at the beginning and end of the allocated memory stack, if at any time the operating system finds these cookies have been over written, the system knows a Buffer Overflow has occurred.
The Russian security group MaxPatrol have actually found a way of bypassing this type of Buffer Overflow protection.
They issued Microsoft with a piece of Proof of Concept code to prove it, Microsoft has since denied the vulnerability exists.
If you wish to have a look at the white paper published by MaxPatrol you can find it here:
http://www.maxpatrol.com/defeating-xpsp2-heap-protection.pdf or the HTML Version:
http://www.maxpatrol.com/defeating-xpsp2-heap-protection.htm
Despite this potential vulnerability, to date no Buffer Overflows have been discovered in Service Pack 2.

**Patch Management:**

In Service Pack 2, by default Windows XP Service Pack 2, will automatically download and Install new Patches and Updates.
It is possible to turn off this feature, if you wish to be in charge of the Installation of patches.
However I would strongly recommend leaving this feature turned on, on all your windows machines.
It is possible to stop the Installation of patches that require reboots while Windows is running, I personally recommend you set Windows to update itself at a time when you're away from your machine, so if it needs to reboot, you won't be doing any work that needs saving at the time.
Beware though, that if you leave your computer on doing something at night, while you have automatic updates turned on, in the morning you may have found your computer rebooted during the night.

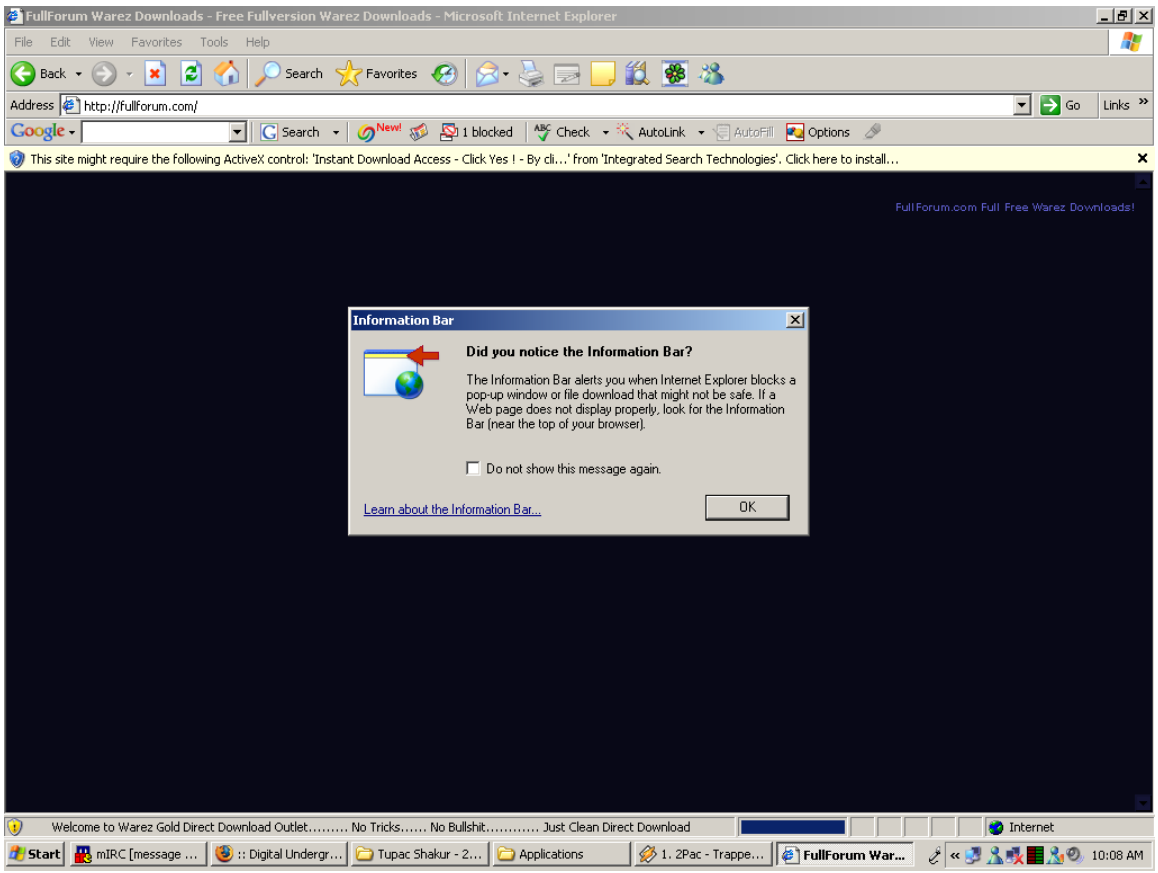
**Internet Explorer Improvements:**

A couple of improvements have been made in Internet Explorer.
The first being, a pop-up blocker which is added to Internet Explorer, to be fair the pop-up stopper is fairly decent and will stop most pop-ups and "pop-unders".
However if your looking to stop **all** pop-ups I would recommend looking for a 3rd party pop-up blocker.
I would have liked it a lot more if Microsoft had allowed more user customization of the pop-up stopper.




**Above is a screenshot, showing the Service Pack 2 pop-up blocker in action.**

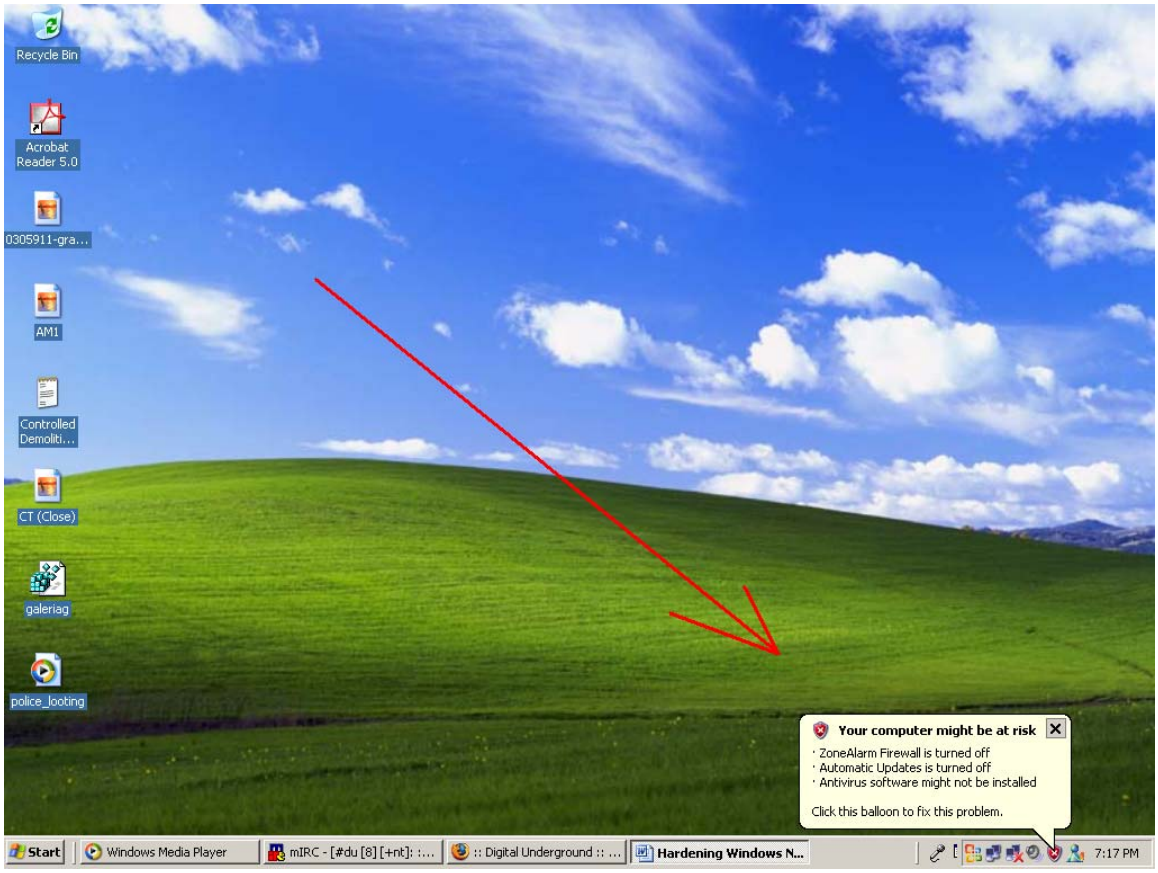
The second and probably one of the most important improvements that comes with SP2, is the fact, that ActiveX is disabled in Service Pack 2.
ActiveX in Service Pack 1 allowed attackers to download, execute and Install unwanted software on a victim's computer.
Since Installing SP2, I noticed the amount of Spyware I was receiving was significantly less than when I had just had SP1 Installed.
However Spyware vendors have found other methods of downloading this malicious content on to people's computer, so beware that SP2 is not protected.
I was disappointed to find out, that Internet Explorer (With SP2) does not feature the Buffer Overflow protection that the Windows operating system features, there have been a few Buffer Overflows in IE6 discovered since the launch of SP2.




**Above is a screenshot asking the user whether or not they want to enable ActiveX.**

## Detection of Anti-Virus Software and Firewall Software:

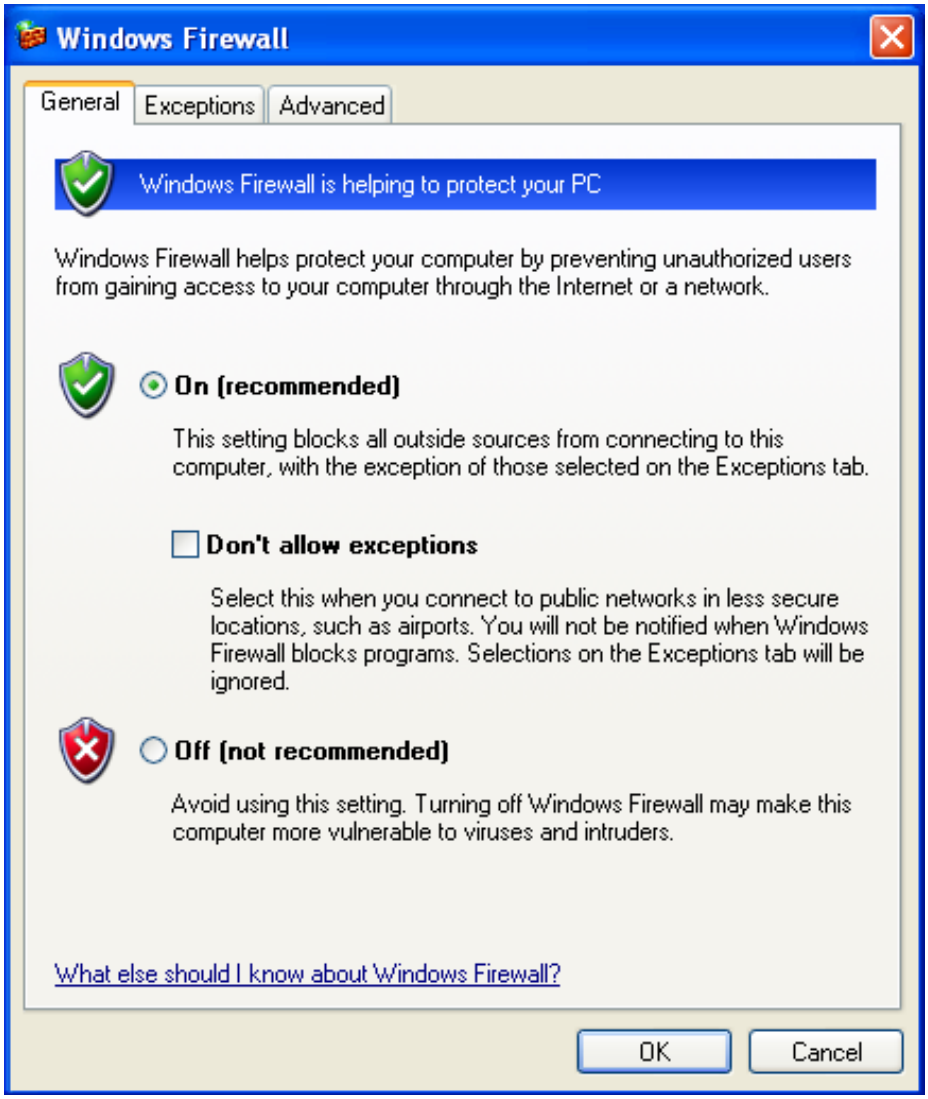
By default SP2 will try and detect whether or not you are currently running Anti-Virus or Firewall software.
If you have an Anti-Virus Installed and it is not currently running SP2 Security Centre will notify you about the fact it is not running, the same applies with a firewall.
At times viruses or Trojans may disable your Anti-Virus or Firewall software, I think this feature of Microsoft's was a good idea.




**Above is a screenshot showing the alert which windows generates after Anti-Virus or Firewall software is disabled.**

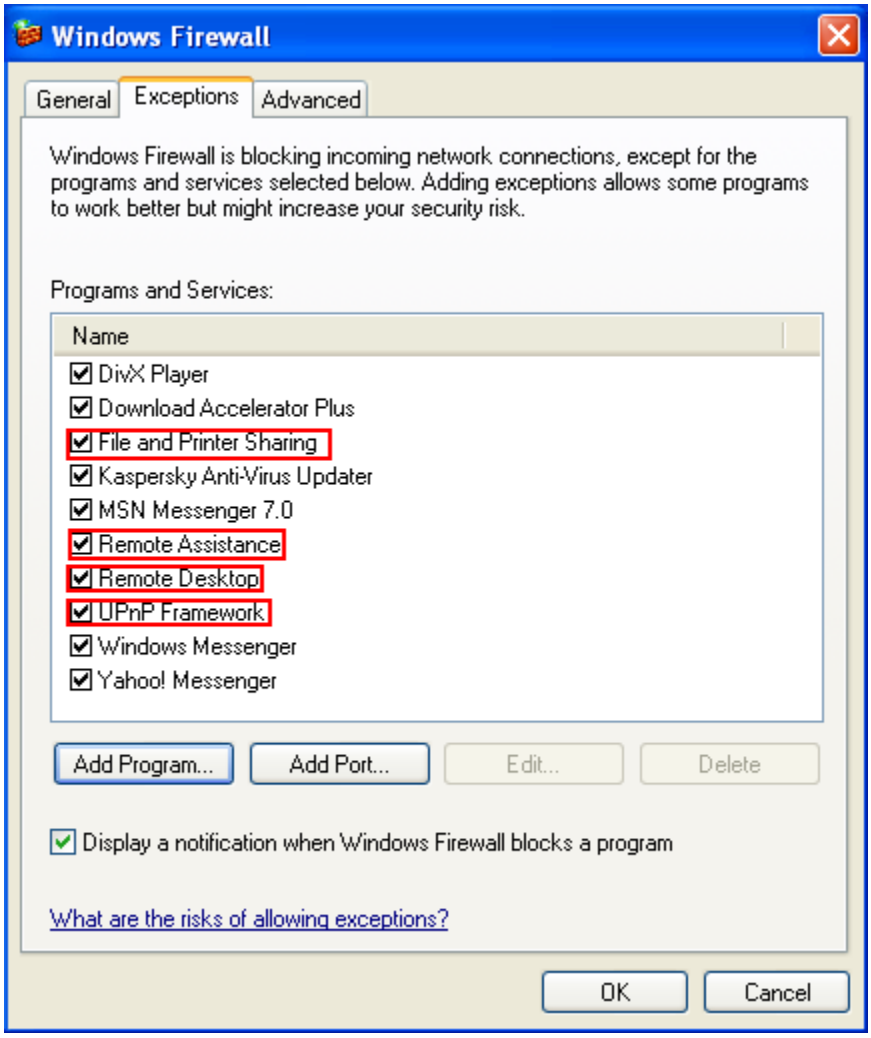
## Service Pack 2 Firewall:

The Service Pack 2 Firewall was possibly one of the best features that came with Service Pack 2.
Unlike with Service Pack 1, the Service Pack 2 firewall is enabled by default and ready to go.



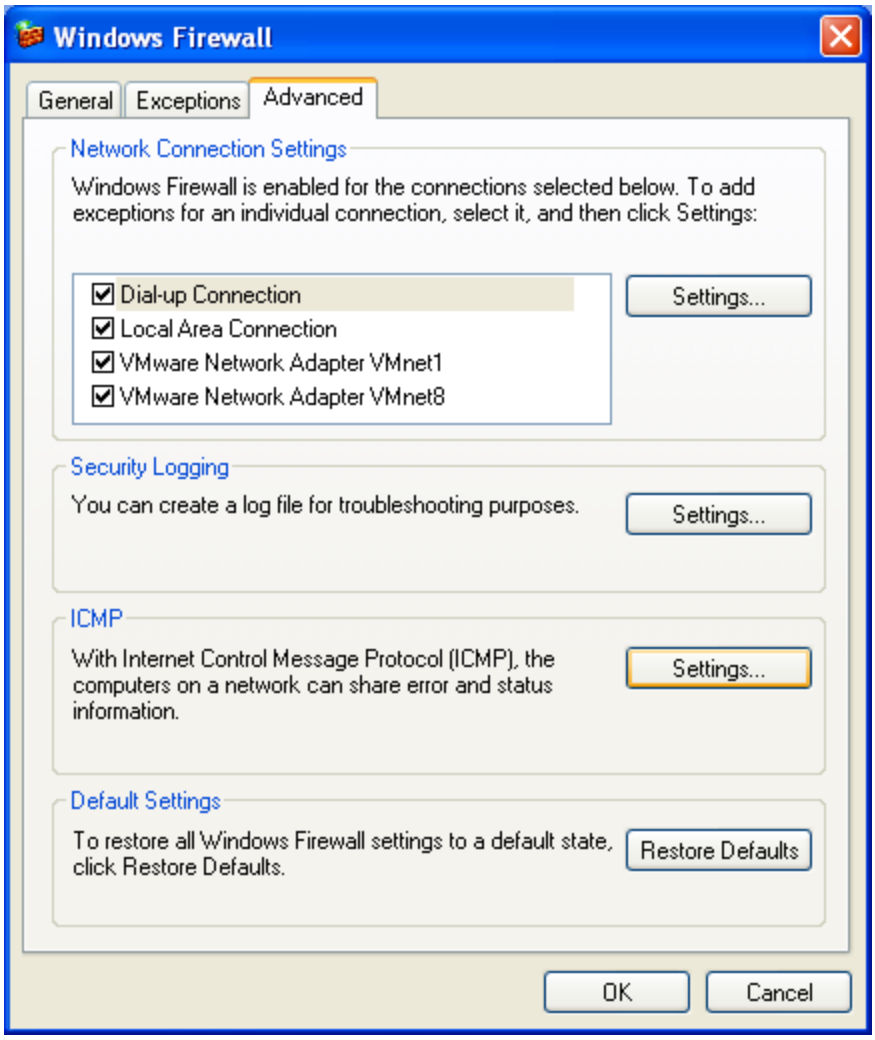

**Above is a screenshot of the Service Pack 2 Firewall.**

By default the Firewall is enabled, and I don't recommend you turn it off, not unless you have a third party firewall.
When I first heard about the Service Pack 2 Firewall, I thought that it would lock down Windows pretty good, worms like msblast and Sasser would have been crippled by this firewall.
When I Installed Service Pack 2, and checked out the Firewall, I was severally disappointed.
By default, the Firewall allows access to a lot of Windows services which are exploitable.

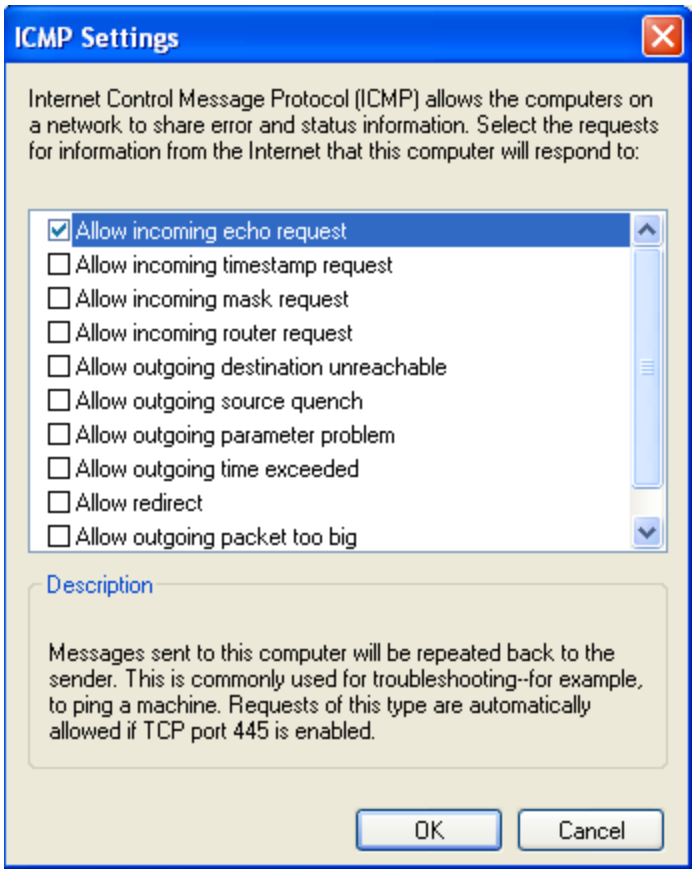



How does Microsoft possibly expect their Firewall to be of any use, if potentially exploitable services are allowed to access the Internet? Does Microsoft expect users to set the firewall to block these services themselves?
If you are going to use the SP2 firewall, as a form of protection I strongly recommend blocking services such as **File and Printer Sharing, Remote Assistance, Remote Desktop and UPnP.**

One thing I think Microsoft may have got right with there Firewall, was the power to restrict the sending and receiving of ICMP Packets.




**Above is a screenshot showing features of the Advanced tab on the SP2 Firewall.**




Which of the following rules you choose to enable is your choice, but if you wish for your machine to be extra secure, think carefully about what rules should be enabled/disabled.

**Viruses Disabling The SP2 Firewall:**

For quite sometime, Trojans that were available on the Internet were able to terminate both Anti-Virus and Software Firewalls, in 2003 most vendors added features to there software which prevented Trojans and other viruses from disabling there software.
However the SP2 Firewall can be easy disabled by quite a simple method (Which I won't bother documenting.)
Microsoft have yet to fix this problem, It seems that Microsoft are sometimes unwilling to accept certain potential vulnerabilities in there operating system.
This is something Microsoft urgently needs to fix.

**Conclusion:**

To sum up what I have gone over, the Service Pack 2 Firewall is a below average Firewall **at best.** I would strongly recommend using a Firewall like **Zone Alarm** or **Sygate.**

# Security Tools:

From time to time our systems get infected with viruses, Trojans and/or Spyware, no matter how secure we think our systems our sometimes we still get infected.
There are numerous tools available freely on the Internet that can assist in the removal of malware.

**PS Tools:**

PS Tools is a command line application that allows you to get detailed information on processes running on your machine, you can also manage these processes.
Viruses often disable or alter Task Manager in Windows, so PS Tools can be very handy to help remove those tricky viruses that even your Anti-Virus has problems with.

http://www.sysinternals.com/Files/PsTools.zip

**SDelete**

SDelete isn't so much a security tool, although it can be.
SDelete is a program used for permanent deletion of files on your hard drive, often this is probably used to get rid of evidence in a crime.
However It can be used legitimately, sometimes sensitive information may be needed to be erased from your hard drive, a skilled attacker may choose to try and recover delete files once he breaks into a machine, using this tool that attacker won't be able to recover sensitive information.

http://www.sysinternals.com/Files/SDelete.zip

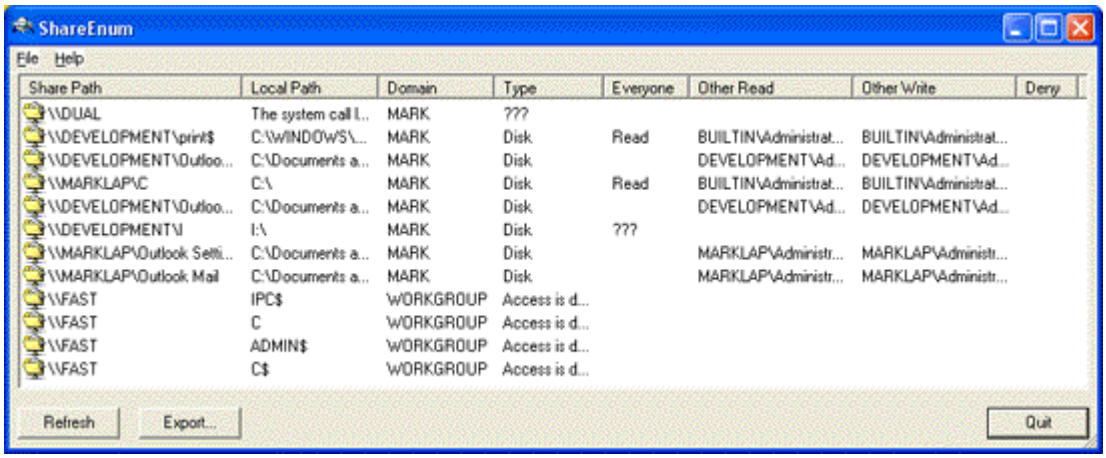
**AutoRuns**

AutoRuns is a program that can show you're a majority of the programs that are set to run on start up, this of course can be especially useful in the removal of malware.

http://www.sysinternals.com/Files/Autoruns.zip

**ShareEnum**

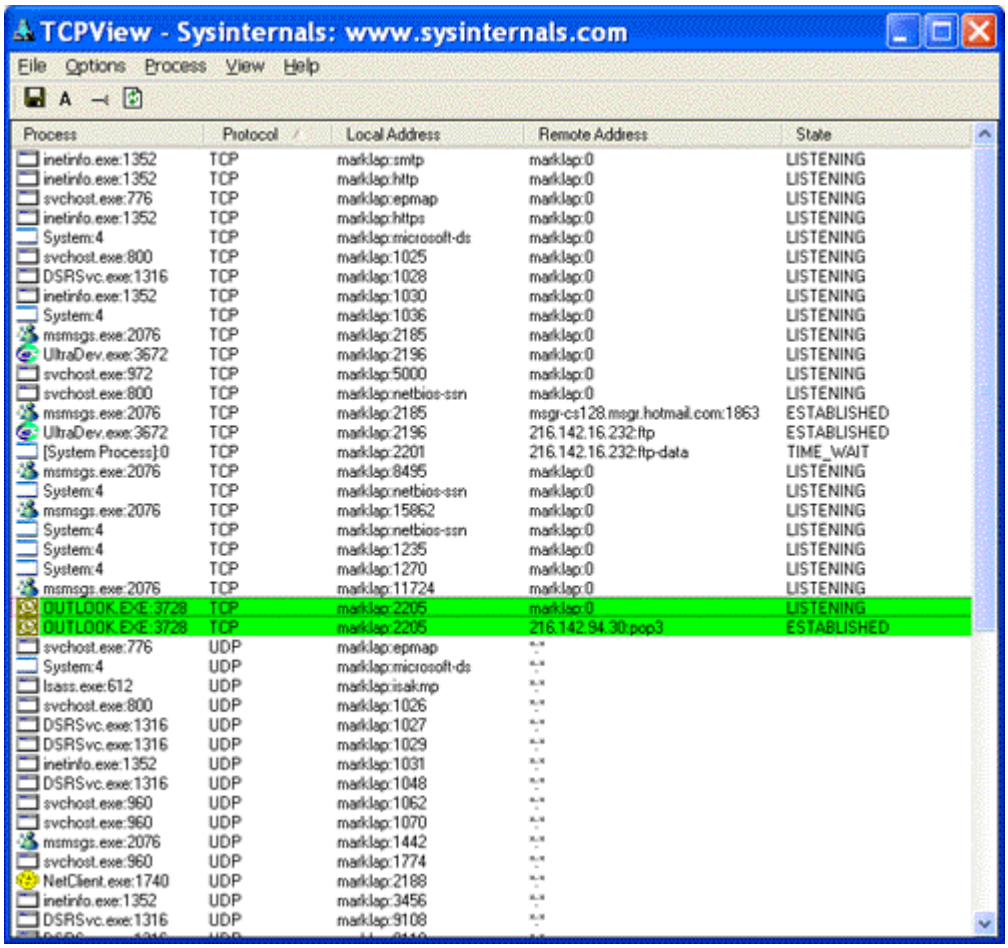
ShareEnum is a tool that can be used to scan your network for network shares, you can also determine the permissions on each of the shares.




http://www.sysinternals.com/Files/ShareEnum.zip

**TCPView**

TCPView is similar to netstat, it allows you to see a detailed list of TCP and UDP connections on your machine, this will be useful if a virus has disabled your command prompt and you are unable to use netstat.




http://www.sysinternals.com/Files/TcpView.zip

**PendMoves**

PendMoves is a program that can be used to rename or delete files after reboot, this is especially useful for malware that cannot be deleted while it's running.

http://www.sysinternals.com/Files/PendMoves.zip

# About The Author:

I (Aelphaeis Mangarae) am an Administrator at SecurZone.
– http://SecurZone.org
SecurZone is a security portal where both Beginners and Professional security enthusiasts discuss IT Security.
I am also a moderator at the Zone-H forums.
- http://forum.zone-h.org
Email: adm1n1strat10n AT hotmail DOT com
MSN: adm1n1strat10n AT hotmail DOT com
IRC: irc.igs.ca:6667 #d-u

# Greetz To:

htek, HackJoeSite, FRSilent, Read101, Syst3m Of Cha0s, The Goon Squad, Media Assasins, tomchu, nic`, r0rkty, Nitrous, SyS64738, Trash-80, morning_wood, snkenjoi, Astharot, Fauley, Furax, PsAuX, SecurityWireless, SysSpider, Siegfried, fritz, darkt3ch, Predator, Alchemist, BioHunter, Dark Sheep, Splinter, digital-flow, butthead, spiderlance, FishNET, W--, nrs, IBMWarpst, Nixus, varu, z16bitseg, jMu, JWT, felosi, ASO, Mega~biTe, wicked, Palmeiro, Kadafiu, h4cky0u & rat_hack.

htek – Where have you been? If your reading this now how about getting into contact with me? I would very much to like to talk to you again.

Syst3m Of Cha0s – Hello guys, I haven't talked to you in ages, d4rk f0rce where did you disappear to?

Alchemist – Start coding CIA again and come back to the Trojan/RAT scene, we are all missing you!

SysSpider – Thanks for helping out with the editing of this paper.