United States Army Signal Center and Fort Gordon
Leader College for Information Technology
School of Information Technology

Information Assurance Division

# Windows®
# System Administrator
# Security Course

7 July, 2005

**TABLE OF CONTENTS**

## Section 1 – Security Threats

Threats are the potential that an existing vulnerability can be exploited to compromise the security of systems or networks. Even if the vulnerability is not known, it represents a threat by this definition.  There are many possible threats. Possible threats include spyware, adware, malware, phishing, system vulnerabilities, and insider threats.

## Spyware

Spyware is any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses, passwords and even credit card numbers.

Spyware is similar to a Trojan horse in that users unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today. Aside from the questions of ethics and privacy, spyware steals from the user by using the computer's memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's Internet connection. Because spyware is using memory and system resources, the applications running in the background can lead to system crashes or general system instability.

Because spyware exists as independent executable programs, they have the ability to monitor keystrokes, scan files on the hard drive, snoop other applications, such as chat programs or word processors, install other spyware programs, read cookies, change the default home page on the Web browser, consistently relaying this information back to the spyware author who will either use it for advertising/marketing purposes or sell the information to another party. Licensing agreements that accompany software downloads sometimes warn the user that a spyware program will be installed along with the requested software, but the licensing agreements may not always be read completely because the notice of a spyware installation is often couched in obtuse, hard-to-read legal disclaimers. Some of the more popular spyware are *Bonzi Buddy, Bargain Buddy, Comet Cursors, eZula HotText, Gator, GoHip, Lookfor.cc, Radiate, WebHancer, and WildTangent.*

Anti-spyware software can stop and remove spyware.  As Spyware is constantly changing and evolving there's no one effective method in identifying and tracking Spyware. Good anti-Spyware software should take several different approaches

as a layered approached to entrapping Spyware has been proven to be far more effective than a single line of defense. Three most effective layers of Spyware detection are:

Name Matching – Names of a known Spyware files are stored in anti-Spyware definitions database and during the scan process, files with the same filename are reported to the user as Spyware.

This method, although effective can be dangerous when used across the board for all filenames, because some malicious applications have the same filenames as useful files, which can cause dangerous "false positives". And if a lesser anti-Spyware programs release spyware files named "word.exe" or "outlook.exe" it will blindly delete programs improperly identified as Spyware.

Entire File Signature Matching – is a method where a digital signature of a known Spyware file is stored in the anti-Spyware definitions. If a file is found with the same signature, the file is reported to the user as being Spyware. There are no "false positive" with this method as the program is looking at the contents of the file, not just the filename.

Code-Based Detection – is a method that stores actual detection and removal code in the definition files which can include using the above two methods to detect and remove spyware. Typically this approach is used for more complex types of Spyware that dynamically change their size for each installation, presumably to avoid detection.

**Adware**

Adware is any software application in which advertising banners are displayed while the program is running.  Adware is also a form of spyware that collects information about the user in order to display advertisements in the web browser based on the information it collects from the user's browsing patterns.  Software can be Adware and Spyware at the same time.  If an advertisement banner (adware) sends data back to a third party without asking the user (spyware), then it is both adware and spyware.

Adware contains banner advertisements that create revenue for the company. Adware installs components on your computer that will send marketing information whenever you are online. Unlike Spyware, adware contains a disclosure telling you that they will be using your information. It is important to read the privacy policy when downloading adware.

**Malware**

Malware is the abbreviation for malicious software.  It is a software that is designed specifically to damage or disrupt a computer system such as virus or

trojan horse.  Malware can be classified based on how it is executed, how it spreads, and how it operates.  The many different types of Malware includes:

Virus: a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

Computer Worms – Worms are similar to viruses but are stand-alone software and thus do not require host files (or other types of host code) to spread themselves. They do modify their host operating system, however, at least to the extent that they are started as part of the boot process. To spread, worms either exploit some vulnerability of the target system or use some kind of social engineering to trick users into executing them.

Trojan – Trojan horse program is a harmful piece of software that is disguised as legitimate software. Trojan horses cannot replicate themselves, in contrast to viruses or worms. A trojan horse can be deliberately attached to otherwise useful software by a programmer, or it can be spread by tricking users into believing that it is useful. To complicate matters, some trojan horses can spread or activate other malware, such as viruses.

Backdoor – Backdoor is a  piece of software that allows access to the computer system bypassing the normal authentication procedures. Based on how they work and spread, there are two groups of backdoors. The first group works much like a Trojan, i.e., they are manually inserted into another piece of software, executed via their host software and spread by their host software being installed. The second group works more like a worm in that they get executed as part of the boot process and are usually spread by worms carrying them as their payload.

Rootkits – Rootkit is software inserted onto a computer system after an attacker has gained control of the system. Rootkits often include functions to hide the traces of the attack, as by deleting log entries or cloaking the attacker's processes. Rootkits may also include backdoors, allowing the attacker to easily regain access later; or exploit software to attack other systems. Because they often hook into the operating system at the kernel level to hide their presence rootkits can be very hard to detect.

**Phishing**

Phishing is the act of sending e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering

private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information. For example, 2003 saw the proliferation of a phishing scam in which users received e-mails supposedly from eBay claiming that the user's account was about to be suspended unless he clicked on the provided link and updated the credit card information that the genuine eBay already had. Because it is relatively simple to make a Web site look like a legitimate organizations site by mimicking the HTML code, the scam counted on people being tricked into thinking they were actually being contacted by eBay and were subsequently going to eBay's site to update their account information. By spamming large groups of people, the "phisher" counted on the e-mail being read by a percentage of people who actually had listed credit card numbers with eBay legitimately.

If you get an email or pop-up message that asks for personal or financial information, do not reply or click on the link in the message. Legitimate companies don't ask for this information via email. If you are concerned about your account, contact the organization in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address. In any case, don't cut and paste the link in the message.

Don't email personal or financial information. Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's Web site, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.

Review credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.

Use anti-virus software and keep it up to date. Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge. Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for anti-virus software that recognizes current viruses as well as older ones; that can effectively reverse the damage; and that updates automatically.

**System Vulnerabilities**

System vulnerabilities are weaknesses in the software or hardware on a computer system that can be exploited to gain access to or shut down a network. Attackers take the easiest and most convenient route and exploit the best-known flaws with the most effective and widely available attack tools.  They rely on system administrators not changing the default setting or not keeping their systems up-to-date with the latest patches.  The SysAdmin, Audit, Network, Security (SANS) Institute comprises a list of the top vulnerabilities in computer systems.  The following is the top ten vulnerabilities and a brief description to Windows Systems:

**Web Server & Services**

Description:
Default installations of various HTTP servers and additional components for serving HTTP requests as well as streaming media to the internet from Windows platforms have proven vulnerable to a number of serious attacks over time. The impact of these vulnerabilities can include: denial of service, exposure or compromise of sensitive files or data, execution of arbitrary commands on the server, and complete compromise of the server.

HTTP servers including IIS, Apache, and iPlanet (now SunOne) have had numerous issues that have been patched as they have been discovered. Ensure that all patches are up to date for the server and that a current version is running. In most HTTP server software the default configuration is rather open leaving large avenues for exploit. Whilst this has been changed to a 'secure by default' posture for IIS 6.0, it is crucial that administrators take the time to fully understand their web server and adjust the configuration to allow only those features and services required.

Most web servers include sample applications or web sites that were designed to demonstrate the functionality of the web server. These applications were not designed to operate securely in a production environment. Versions of IIS before 6.0 include sample applications that can be exploited to allow remote viewing or overwriting of arbitrary files as well as remote access to other sensitive server information, such as system configuration settings and paths to binaries. Remove these applications prior to placing the server into production.

Third-party web add-ons such as ColdFusion and php can introduce further vulnerabilities in a webserver installation, either through misconfiguration or through vulnerabilities inherent in the product.

Operating Systems Affected:
Any Microsoft Windows system with a web server installed could be affected. This includes, but is not limited to: Microsoft IIS: Windows NT4.0 and above, including XP Professional Apache HTTP server: Windows NT4.0 SP3 and above are supported, though it is believed to run on Win95 and Win98 Sun Java System/Sun One/iPlanet Web Server: Windows NT4.0 SP6 and above

**Workstation Service**

Description:
Windows Workstation service is responsible for processing user requests to access resources such as files and printers. The service determines if the resource resides on the local system or on a network share, and routes the user requests appropriately.

The network management functions provided by the service can be invoked via any of the following mechanisms.
DCE/RPC calls over SMB protocol after connecting to the service using \\pipe\wkssvc named pipe.
DCE/RPC calls directly over a UDP port (> 1024)
DCE/RPC calls directly over a TCP port (> 1024)
    *Note that the service binds to the first available TCP and UDP port over 1024.*

The Workstation service contains a stack-based buffer overflow that can be triggered by a specially crafted DCE/RPC call. The problem arises because parameters are passed to the logging function without any bounds checking. This overflow can be exploited by an unauthenticated remote attacker to execute arbitrary code on the vulnerable Windows machine with "SYSTEM" privileges. The attacker can obtain complete control of the compromised machine. The exploit code for leveraging the vulnerability has been posted to the Internet and was re-used in some variants of Phatbot/Gaobot worm that infected millions of systems world-wide.

Operating Systems Affected:
Windows 2000 SP2, SP3 and SP4
Windows XP, Windows XP SP1
Windows XP 64 Bit Edition

**Windows Remote Access Services**

The family of Windows Operating systems supports a variety of different networking methods and technologies. There is native support for most industry standard networking protocols and built-in functionality for many Microsoft specific networking methods and techniques. Common avenues for exploitation include Network Shares, Anonymous Logon, remote registry access, and remote

procedure calls.

***NETBIOS*** - A set of API's (application program interface) that can allow the sharing files or folders across a network with other hosts through Windows network shares. The underlying mechanism of this feature is the Server Message Block (SMB) protocol, or the Common Internet File System (CIFS). These protocols permit a host to manipulate remote files just as if they were local.

Although this is a powerful and useful feature of Windows, improper configuration of network shares may expose critical system files or may provide a mechanism for a nefarious user or program to take full control of the host. Many computer owners unknowingly open their systems to hackers when they try to improve convenience for co-workers and outside researchers by making their drives readable and writeable by network users.

***Anonymous Logon*** - An anonymous session is a communication link established without correct credentials (i.e. blank username and password). Null sessions can be used to display information about users, groups, shares and password policies. Windows 2000 and later services running as the Local System account on the local computer use the local computer account to authenticate to other servers.

***Remote Registry Access*** - Microsoft Windows 9x, Windows CE, Windows NT, Windows 2000, Windows 2003, Windows ME and Windows XP employ a central hierarchical database, known as the Registry, to manage software, device configurations, and user settings. Improper permissions or security settings can permit remote registry access or execution of code or applications that should not be allowed to run.

***Remote Procedure Calls*** - All versions of Microsoft operating systems (Windows NT 4.0, 2000, XP, and 2003) provide an inter-process communication mechanism that allows programs running on one host to execute code on remote hosts. Three vulnerabilities have been published that would allow an attacker to run arbitrary code on susceptible hosts with Local System privileges. One of these vulnerabilities was exploited by Blaster/MSblast/LovSAN and Nachi/Welchia worms. There are also other vulnerabilities that would allow attackers to mount Denial of Service attacks against RPC components.

Operating Systems Affected:
Windows 95, Windows 98, Windows NT Workstation and Server, Windows Me, Windows 2000 Workstation and Server, Windows XP Home and Professional, and Windows 2003 are all potentially vulnerable.

<u>Microsoft SQL Server (MSSQL)</u>

Description
The Microsoft SQL Server (MSSQL) contains several serious vulnerabilities that allow remote attackers to obtain sensitive information, alter database content, compromise SQL servers, and, in some configurations, compromise server hosts.

MSSQL vulnerabilities are well-publicized and actively under attack. Two recent MSSQL worms in May 2002 (SQLSnake/Spida Worm) and January 2003 (SQL-Slammer/SQL-Hell/Sapphire Worm) exploited several known MSSQL flaws. Hosts compromised by these worms generate a damaging level of network traffic when they scan for other vulnerable hosts.

Operating Systems Affected:
Any Microsoft Windows system with Microsoft SQL/MSDE Server 7.0, Microsoft SQL/MSDE Server 2000 or Microsoft SQL/MSDE Server Desktop Engine 2000 installed, as well as any system, which uses the MSDE engine separately.

**Windows Authentication**

Description:
Passwords, pass-phrases and security codes are used in virtually every interaction between users and information systems. Most forms of user authentication, as well as file and data protection, rely on user-supplied passwords. Since properly authenticated access is often not logged, or even if logged not likely to arouse suspicion, a compromised password is an opportunity to explore a system from the inside virtually undetected. An attacker would have complete access to any resources available to that user, and would be significantly closer to being able to access other accounts, nearby machines, and perhaps even administrative privileges. Despite this threat, accounts with bad or empty passwords remain extremely common, and organizations with good password policy are far too rare.

The most common password vulnerabilities are:
User accounts have weak or nonexistent passwords.
Regardless of the strength of their password, users fail to protect it.
The operating system or third-party applications create accounts with weak or nonexistent passwords.
In many commercial and Open Source applications, the hashing algorithms is known and often the hashes are stored where they can be accessed by standard users. Whilst system policies cannot help protect against hashing implementations or short-comings, the use of strong passwords can help thwart attacks against the hashes to recover the pass-phrase.

Operating Systems Affected:
All Microsoft Windows operating systems.

**Web Browsers**

The Browser is the means by which computer users access the web on Microsoft Windows systems. The dominant web browser is Microsoft Internet Explorer (IE), which is the default web browser installed on Microsoft Windows platforms. Other Web browsers include Mozilla, Firefox, Netscape and Opera. The latest version of IE is 6, and the **US-CERT** has issued an advisory outlining the security enhancements and features available in IE 6. The vulnerabilities discussed here are also applicable to Mozilla versions 1.4 - 1.7.1, Firefox version 0.9.x, Netscape version 7.x, and Opera version 7.x.

The problems are six-fold:

- Large Number of vulnerabilities over the last few years in comparison to other browsers - 153 IE vulnerabilities since April 2001, according to the **Security Focus Archive**.
- Longer Time to patch known IE vulnerabilities - Users have had to wait in excess of six months from the time the vulnerability is disclosed before Microsoft issues a patch.
- Active X and Active Scripting controls themselves have not been found to be open to particular exploitation, but can be used to bypass the security constructs of the browser and potentially impact upon the host system.
- Large number of unpatched vulnerabilities - 34, according to **http://umbrella.name/**
- Spyware/Adware vulnerabilities - This affects all browsers and systems that facilitate access and use of web resources.
- Integration of IE browser into the Operating System, which makes the OS more vulnerable to exploitation.

Operating Systems Affected:
These vulnerabilities exist on Microsoft Windows systems running any version of these browsers. It is important to note that IE is installed with a wide variety of Microsoft software and is therefore typically present on all Windows systems, even though the user may not wish it installed or utilized. All other browsers are installed at the user's discretion and the user decides whether the browser is used by other applications.

**File Sharing Applications**

Description
Peer to Peer File Sharing Programs (P2P) are used by a rapidly growing user base. These applications are used to download, and distribute many types of data (e.g. music, video, graphics, text, source code, and proprietary information to name a few). P2P applications have a number of legitimate uses, including the distribution of OpenSource/GPL binaries, ISO images of bootable Linux distributions, independent artists' creations, and even commercial media such as film trailers and game previews. Other times, the data is either of a questionable nature or is copyrighted. With the legal troubles experienced by Napster, the majority of these P2P programs now operate through a distributed network of clients, sharing directories of files or entire hard drives of data. Users can enter search parameters through the client software, and then one or more channels of communication are opened between participants as the client software contacts other network participants to locate the desired file. Clients participate by downloading files from other users, making their data available to others, and in some models by functioning as super-nodes which can coordinate searches for multiple users. Peer to Peer communication consists of get requests, replies, and file transfers. A participant can concurrently perform multiple downloads while also serving multiple uploads. Searches for content can use almost any text string the user can conceive. Most of these programs currently use default ports, but can automatically or manually be set to use different ports if necessary to circumvent detection, firewalls, or egress filters.

Operating Systems Affected:
There are versions of P2P software available for all Windows operating systems currently in use, along with versions for UNIX and Linux systems.

**LSAS Exposures**

Description:
The Windows Local Security Authority Subsystem Service on Windows 2000, Server 2003 and Server 2003 64 Bit, XP and XP 64 Bit editions contains a critical buffer overflow that if exploited can lead to full system compromise. This overflow is outlined in the Microsoft Security Bulletin MS04-011. This attack can be accomplished remotely and anonymously over RPC on un-patched Windows 2000 and XP systems but requires administrative privileges to be effective.

Operating Systems Affected:
Windows 2000, Windows XP and Professional, Windows XP 64-Bit Edition, Windows 2003

**Mail Client**

Description:
Microsoft Outlook is a personal information manager and email client program for Microsoft Windows. It is primarily an e-mail application, though it also provides calendar, task and contact management. When used in conjunction with a Microsoft Exchange Server, Microsoft Outlook can provide additional groupware functionality, such as supporting multiple users, helping to co-ordinate meeting times, and providing shared calendars and mailboxes.

Outlook Express (OE) is a basic email & contact management client, bundled with Internet Explorer since the earliest versions - which itself has been an integral part of all versions of Microsoft Windows starting with Windows 95. The most current version of Outlook Express, 6.0 with SP1 applied, is available as a free download from Microsoft. By integrating products such as Internet Explorer and Outlook Express into other product lines, including Office, BackOffice, and the Windows operating system, Microsoft has allowed for common technologies and code to be used across the platform. Unfortunately, this practice also introduces single points of failure and heightens the impact that any single security vulnerability may pose.

One of Microsoft's goals has been to develop a usable and intuitive email and information management solution. Unfortunately, the embedded automation features are at odds with the built-in security controls (often disregarded by end-users). This has given rise to e-mail viruses, worms, malicious code to compromise the local system, and many other forms of attack.

Potential security threats of email clients include:
- Infection of computer with virus or worm - malicious code which spreads through attachments or embedded scripting in a message body;
- Spam - unsolicited commercial e-mail;
- Web beaconing - validation of email addresses triggered by opening of message by recipient.

Operating Systems Affected:
All versions of Microsoft Windows come with Outlook Express bundled with Internet Explorer, and are therefore potentially vulnerable.

**Instant Messaging**

Description
Instant Messaging technology has matured over the last few years from a novel add on application that enabled users to quickly stay in touch with friends and

family, to a core Windows Operating System capability often used for business communication, collaboration, and operational support. While third party Instant Messaging (IM) applications still hold a large share of IM deployments, there is a growing trend to integrate Messaging functionality into the Operating System itself which can potentially pose a direct security threat to organizations that have acceptable use policies or secure operational frameworks that deny the use of this technology. The discovery of vulnerabilities in these programs also poses a significant risk to organizations that lack the technical countermeasures, security staff, or capabilities to mitigate this increasingly embedded threat.

By far, a great majority of IM applications found on Windows systems are Yahoo! Messenger (YM), AOL Instant Messenger (AIM), MSN Messenger (MSN) and Windows Messenger (WM), which is now fully integrated into Windows XP Professional and Home Editions. The capabilities that these programs bring to the desktop are wide ranging and may provide users with the ability to check remote web based email, do voice chat, perform video communication, and send and share data files above and beyond simple text based chatting. There is also a growing trend of "multi network" messaging programs that provide the user with a centralized interface to disparate messaging networks and protocols, like Trillian and the recently formed AOL, Yahoo!, and MSN chat alliance, which enabled all three clients to interact seamlessly in the workplace.

Remotely exploitable vulnerabilities in these programs or associated dependencies are a growing threat to the integrity and security of networks, directly proportional to their rapid integration and deployment on Windows systems. Attack scenarios for Instant Messaging vulnerabilities are widely varied, and can come in the form of remotely executed buffer overflows (RPC based, packet malformation), URI/malicious link based attacks, file-transferring vulnerabilities, and Active X exploits.

Vulnerabilities in these programs typically arise from the following categories: Outdated ActiveX controls - e.g. MSN Messenger "ResDLL" Buffer Overflow, Yahoo! Voice Chat ActiveX Control Buffer Overflow Vulnerability), Yahoo! Webcam ActiveX Control Buffer Overrun Vulnerability).  URI implementation problems - e.g. Yahoo! Messenger malicious script execution and Yahoo! Messenger URI handler buffer overflow.  Various Buffer Overflows, such as those resulting from file transfers. - e.g.MSN Messenger file validation failure, Yahoo! Messenger "Imvironment" and "message" field buffer overflows respectively, AOL Instant Messenger TLV 0x2711 packet parsing buffer overflow, Yahoo! Messenger YAuto.DLL Open Buffer Overflow Vulnerability, AOL Instant Messenger Getfile Screenname Buffer Overrun Vulnerability)

These applications not only introduce network-based vulnerabilities into systems but also pose an intellectual property loss risk, potential for loss of confidentiality, and threat of employee productivity loss. While mitigating remotely exploitable weaknesses in these programs is of utmost importance, the necessary

acceptable use policy and ingress/egress traffic enforcement is also of paramount importance to ensure one avoids the problems that Instant Messaging can introduce into a network.

Operating Systems Affected:
Windows 98, Windows ME, Widows 2000 and Professional, Windows XP and Windows 2003 are capable of running the Microsoft Instant Messenger. All versions of Microsoft Windows XP come with Instant Messenger bundled with operating system.

You can reference more information on top vulnerabilities to Windows System on website **http://www.sans.org/top20/**.

## Insider Threats

Internal attacks represent a serious threat today: computers can get easily compromised; laptops or other wireless devices can get stolen. Once a machine, or several of them are compromised and controlled by an attacker, they can exhibit a subjective behavior. Most surveys have shown that insiders -- people with authorized access to a computer network, do the most damage. Many insiders have the access and knowledge to compromise or shut down entire systems and networks.  In many cases, acts of computer sabotage and extortion—like violence in the workplace—have been committed by disgruntled employees who are angry about lay-offs, transfers, and other perceived grievances. Other cases involve employees who take advantage of their position of trust for financial gain, hackers who are employed within the critical infrastructure caught engaging in unauthorized explorations, and "well-motivated" employees who claim they are acting in the best interest of their organizations. Other perpetrators include "moles," individuals who enter an organization with the explicit intent to commit espionage, fraud or embezzlement. Overall, case investigators report that the number of computer-related offenses committed by insiders is rising rapidly each year.

Not taking these possible threats seriously and securing your computer systems will not only result in a possible denial of service, but also severe financial loss. The following statistics is USA Today about the well-known Malware damages that have occurred in the last five years:

Malware damage estimates (USA Today)

| 1999 | Melissa virus | $80 million |
|------|---------------|-------------|
| 2000 | Love Bug Virus | $10 billion |
| 2001 | Code Red ½ worms | $2.6 billion |
| 2001 | Nimda virus | $590 million to $2 billion |
| 2002 | Klez worm | $9 billion |

2003 Slammer worm                    $1 billion

More statistics from Gartner Group.

- Conservatively estimates that the hourly computer outage cost is in the neighborhood of $42,000 Average downtime for a company is 175 hours a year.

- Estimates there are 600 website compromises per day

- In 2003 there were 215,000 identity theft reports in the U.S. totally $437 million

- Spam accounts for 52 percent of all email at a corporate cost of $41.6 billion

- Internet fraud complaints roste to 48,252 by 2002

- Verisign reports 6.2 percent of all e-commerce transactions were fraudulent with the U.S. having 47.8 percent of the world total

- In 2002, businesses spent 12% of the IT budget on security

- Hacker insurance is expected to be a $900 million market by the end of 2005

**Section 2 – Regulations, Standards, Policies, Best Practices for Information Assurance**

**What is Information Assurance?**

Information Assurance (IA) is defined as measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information assurance is a relatively new discipline that was established in the late 1990s. It combines the older disciplines of Information Security (INFOSEC), Communications Security (COMSEC), and Computer Security (COMPUSEC), as well as new missions such as Computer Network Defense (CND). It is also a very dynamic discipline that is driven by the rapid emergence of the Global Information Grid (GIG), rapidly changing technology, and rapidly evolving threat. It is a discipline composed of many roles – from senior executives to system administrators to system users. While it will never be possible to consolidate all IA guidance into a single reference, a great deal of effort is being expended to develop a policy framework in the form of the Department of Defense (DoD) 85xx series of issuances. Eventually, we may achieve a comprehensive reference framework.

**Guidelines that govern Information Assurance**

**AR 25-1 Army Knowledge Management & Information Technology Management**

This regulation establishes the policies and assigns responsibilities for information management and information technology. It applies to information technology contained in both business systems and national security systems developed for or purchased by the Department of Army. It addresses the management of information as an Army resource, the technology supporting information requirements, the resources supporting information technology, and Army Knowledge Management as a means to achieve a knowledge-based force. Latest publication is dated 30 June 2004.

**AR 25-2 Information Assurance**

This regulation provides Information Assurance policy and mandates procedures for implementing the Army Information Assurance Program, consistent with today's technological advancements, in a generic fashion to avoid dependency on specific technology. It establishes policies and assigns responsibilities for achieving acceptable levels of Information Assurance in engineering,

implementation, operation, and maintenance for all information systems connecting to or crossing any U.S. Army-managed network. It provides administrative and systems security requirements, including those for interconnected systems. It defines and mandates the use of risk assessments and the **Defense in Depth Strategy**. It describes the roles and responsibilities of the individuals who constitute the Information Assurance security community and its users, and outlines training and certification requirements. It requires a life-cycle management approach to implementing Information Assurance requirements and requires the implementation of a configuration management process. It establishes a procedure to document the status of generic accreditations for all information systems fielded by Department of the Army organizations, DA-chartered program managers, and Headquarters, Department of the Army staff proponents. It also establishes requirements to ensure that Department of Defense and Army-level designated approving authorities meet the system accreditation policies of this regulation before fielding or testing any system that requires connection to a military network. The latest publication is dated 14 November 2003 and it replaces AR 380-19.  These regulations may be referenced on your SA/NM Course CD or on the web at various sites.  One reference site is http://iase.disa.mil/policy.html#Army.

**AR 380-5 Department of the Army Information Security Program**

This regulation establishes a system for classification, downgrading, and declassification of information; sets forth policies and procedures to safeguard such information; and provides for oversight and administrative sanctions for violations. This regulation gives instructions and assigns responsibilities for the effective implementation and application of Department of Defense Information Security Program policies at all levels of DA. This regulation also gives guidance to physical security and implementation of warning banners.

**AR 380-53 Information Systems Security Monitoring**

This regulation sets forth responsibilities, policy, and procedures for conducting Information Systems Security Monitoring within the U.S. Army. It also provides guidance for U.S. Army elements conducting Information Systems Security Monitoring in support of joint and combined operations and activities. This regulation also gives guidance to the implementation of warning banners.

**Security Configuration Guides and Security Technical Implementation Guides (STIGs)**

The STIGs and NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems. STIGs and NSA Guides are currently being used throughout the government and by numerous entities as a security baseline for their IA systems. STIGs are checklists with settings and option selections that minimize the security risks associated with each computer hardware or software

system that, or is likely to become widely used within the Federal Government. NSA security configuration guides cover proprietary and open source software. NSA's work to enhance the security of software is motivated by one simple consideration: use our resources as efficiently as possible to give NSA's customers the best possible security options in the most widely employed products.  You can reference more information on SA/NM Course CD or website https://iase.disa.mil/

**Common Criteria**

Common Criteria is an international set of standards developed allowing a level of standardization for Information Technology, thusly providing a unified baseline. In January 1996, the United States, United Kingdom, Germany, France, Canada, and the Netherlands released a jointly developed evaluation standard for a multi-national marketplace. This standard is known as the "Common Criteria for Information Technology Security Evaluation" (CCITSE) usually referred to as the "Common Criteria" (CC). Common Criteria is used to find requirements for security features that match specific risk assessments and that have rating for those specific features.  It is also used to publish security requirements so that vendors can design products that meet them.

The Common Criteria for Information Technology Security Evaluation (CCITSE) occasionally (and somewhat incorrectly) referred to as the Harmonized Criteria, is a multinational effort to write a successor to the Trusted Computer System Evaluation Criteria (TCSEC) and Information Technology Security Evaluation Criteria (ITSEC) that combines the best aspects of both. The TCSEC is a collection of criteria that was previously used to grade or rate the security offered by a computer system product. ITSEC are European-developed criteria. Its aim is to demonstrate conformance of a product or system (referred to as a target of evaluation, or TOE) against its Security Target.  Reference web http://csrc.nist.gov/cc/.  There is more information on Common Criteria at http://iase.disa.mil/common/index.html.

**Department of Defense Directive 8500 Series**

This directive establishes policy and assigns responsibilities to achieve Department of Defense (DoD) information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare.

This series implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks. They provide end-to-end protection of DoD information and defend DoD information systems and computer networks from unauthorized or malicious activity. They also provide information assurance (IA) situational

awareness and command and control (C2), improve IA processes through integration and create an empowered IA workforce.

DoD has defined three **mission assurance** categories:

- MAC I – High Integrity, High Availability for DoD information systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness.

- MAC II – High Integrity, Medium Availability for DoD information systems handling information that is important to the support of deployed and contingency forces.

- MAC III – Basic Integrity, Basic Availability for DoD information systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term.

A mission assurance category is always teamed with an independent level of confidentiality.  DoD has also defined **three levels of confidentiality**:

- High Confidentiality for systems processing classified information.
- Medium Confidentiality for systems processing sensitive information as defined in DoDD 8500.1.
- Basic Confidentiality for systems processing public information as defined in DoDD 8500.1.

## DODD 8570.1 DoD Information Assurance Training, Certification and Workforce Management

It provides guidance and procedures for the training, certification and workforce management of DoD Information Assurance workforce. It also provides information and guidance on reporting metrics.

## DITSCAP Department of Defense Information Technology Security Certification and Accreditation Process

DoDI 5200.40 establishes a standard DOD-wide process, set of activities, general tasks, and a management structure to certify and accredit Information Systems (IS) that will maintain the Information Assurance and security posture of the Defense Information Infrastructure throughout the life cycle of the system.

Certification is a security analysis is the following areas: Physical, Personnel, Administrative, Information, Information Systems, and Communications.

Accreditation is a formal declaration by the Designated Approving Authority that an IT system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.  DoDD 8510.1-M is the Department of Defense Information Technology Security Certification and Accreditations Process (DITSCAP).

**Information Assurance Vulnerability Management & Asset Vulnerability Tracking Resource**

AR 25-2 (Para 4-24) provides the guidelines for the Information Assurance Vulnerability Management (IAVM) process to ensure compliance. The Army Computer Emergency Response Team (ACERT) and the Army Network Operations and Security Center (ANOSC) are responsible for vulnerability identification, dissemination and acknowledgement of the IAVM.  Within the ANOSC, these responsibilities are assigned to the Technical Analysis Group (TAG).

**IAVAs** (alerts) mandate suspense dates for acknowledgement and compliance and direct corrective actions to negate vulnerabilities.  They may also direct implementation of additional CND (Computer Network Defense) requirements such as unique scanning or mandated software upgrades.  IAVAs are sent when the risk to Army networks is highest.  Ideally, IAVAs have a 30-day suspense.

**IAVBs** (bulletins) establish mandatory suspense dates for acknowledgement yet allow commanders and IA personnel flexibility for implementation of the corrective actions to negate vulnerabilities or implementation of CND requirements. Corrective actions are required to be completed but are not reported.

Information Assurance Technical Tips (**IATTs**) allow commanders and IA personnel flexibility for acknowledgement and implementation to negate vulnerabilities or implement CND requirements. Acknowledgement and compliance is not reported. Corrective actions are required to be completed but not reported.

The DoD-contracted eEye Retina Network Scanner will become an integral part of Army's multi-layered security strategy to manage risks and maintain policy and compliance. The Retina Network Scanner may be used along with the Harris STAT scanner to perform IAVA and Vulnerability Assessments.  Army users may continue to use the Harris STAT scanner, and shall transition to the Retina Scanner as licenses expire.  The NETCOM Information Assurance and Compliance (OIA&C) is linking the Retina Network Scanner to the Asset and Vulnerability Tracking Resource (A&VTR) Database.

To address the Adware/SPYware threat a work group has been established by Joint Task Force – Global Network Operations (JTF-GNO). As information becomes available for dissemination it will be released via listserver message. A message will be released with guidance on the use of a standalone SPYware removal tool.  Organizations are encouraged to restrain considering a purchase of a separate SPYware solution.

## Reporting Chain

The IA **chain for information flow** top to bottom:

- DAA  (Designated Approving Authority)
- IAPM (Information Assurance Program Manager)
- IAM (Information Assurance Manager)
- IASO (Information Assurance Security Officer)
- SA (System Administrator)

The IA **chain for report of incident** bottom to top:

- SA (System Administrator)
- IASO (Information Assurance Security Officer)
- Commander
- IAM (Information Assurance Manager)
- Local R-CERT (Regional Computer Emergency Response Team)
- IAPM (Information Assurance Program Manager)
- DAA  (Designated Approving Authority)

The IAM notify the ACERT or its subordinate CERT of all incidents, including unsuccessful penetration attempts, and request immediate technical assistance. The IASO or IAM should also notify the supporting CID and INSCOM offices if an unauthorized person successfully penetrated the IS. The ACERT website is https://www.acert.1stiocmd.army.mil/.

1st IO CMD
The 1st IO CMD will notify HQ, CID; DISA/Automated Systems Security Incident Support team (ASSIST); and ACCO INSCOM of actual penetrations of Army IS.

CID and INSCOM
The two commands coordinate to determine investigative jurisdiction if there are no indications of FIS involvement.

## Section 3 - PHYSICAL SECURITY

Physical security is an extremely important part of keeping your computers and data secure-- if an experienced hacker can just walk up to your machine, it can be compromised in a matter of minutes. That may seem like a remote threat, but there are other risks—like theft, data loss, and physical damage—that make it important to check your physical security posture for holes. The regulation governing the Army Information Security Program is AR 380-5.

## Server Access

Most large corporations maintain very strict control over who can enter their server rooms. They use card key or keypad systems, log books and human security to limit unauthorized access. Others may have their servers in publicly-accessible areas. Not only does this expose them to malicious attacks, it increases the risk of accidents. If at all possible, sensitive servers should be kept behind a locked door, not just a door with a lock, and access should be limited to a select set of trustworthy administrators. Of course, you shouldn't let security concerns override the environmental requirements of your hardware. For instance, locking a server in a closet prevents malicious users from accessing it, but if not adequately ventilated, the computer will overheat and fail, rendering your security concerns pointless.

## Server Access Vulnerability

Physical access by unauthorized personnel could result in theft of peripherals, denial of service, security overrides via removable media, or miscellaneous tampering. Remember that there is NO security without Physical Security. Access to the interior of the CPU case exposes the computer to theft, sabotage, and reconfiguration.

1. Place the server in a locked room accessible only by trustworthy administrators.

   - Maintain a list of personnel authorized entry
   - Establish key/access control.

2. Physically lock the CPU case

It's a good idea to restrict physical access, and limit potential damage, but *someone's* got to be able to use the computers—you can't keep everyone away from them. The next layer of a good physical security plan is to limit what can be done with the computers.

**Input/Output Devices**

If your system has peripheral devices connected, then it will not take an attacker long to gain access.  Removal or disabling of input devices prevents any one from causing the system to execute programs or load software. As administrator you will be able to enable access when you need it.

1. Remove the Keyboard, mouse, and monitor, if possible.
2. Consider using KVM switches (Short for keyboard, video, mouse switch, a hardware device that enables a single keyboard, video monitor and mouse to control more than one computer one at a time).

**Check equipment for Unauthorized Attached Devices**

Devices can be attached to equipment which can record network transmission, keystrokes, or other information.

1. IT equipment should not have any attached devices or connections that are unknown to the system administrator.  Check network transmission line for additional devices.
2. Check USB, serial, and parallel ports for attached equipment. The USB Flash Drives small size and large storage capacity can make it a dangerous tool in the wrong hands. You don't have to be an administrator to install one of these devices in Windows 2000/XP/2003, and you can't manage USB devices via Group Policy. These devices present two primary threats to your network: the introduction of malicious software and data theft/loss. And short of disabling all of the USB ports in your environment, they are impossible to defend against.

**Smart Card Readers**

Equipment must be in place before advanced authentication methods can be utilized.

- Install Smart Card readers to enable advanced authentication techniques.

**Boot Sequence**

An operating system can be rebooted using removable media. Once rebooted, the operating system can be modified or reinstalled, overriding password controls. This setting controls the order that the BIOS uses to look for a boot device from which to load the operating system. Configure the BIOS not to boot from the floppy drive or CDROM. This makes it harder for an intruder to remove passwords and account data from your system's disks.

> Change the Boot sequence (in the CMOS).

- Change boot sequence to Hard drive, CDROM, then Floppy. For complete safety, change it so only the hard drive is available for boot.

**Note:** Most personal computers today can start a number of different operating systems. For example, if normally Windows is started from the C: drive, another version of Windows could be selected from another drive, including a floppy drive or CD-ROM drive. If this happens, security precautions taken within the default version of the initial Windows boot might be circumvented. In general, install only those operating systems required. For a highly secure system, this will probably mean installing one version of Windows and ensuring that all partitions are NTFS volumes.

**CMOS Passwords**

Access to the CMOS enables changing of the boot sequence order. Changing the boot sequence can enable reboot via removable media. This is an effective way to prevent unauthorized booting or starting of the computer.

- Install a CMOS password.

**Syskey**

To provide a greater level of protection for master keys and various other secrets use the system key. The system key protects the following sensitive information:

- Master keys that are used to protect private keys
- Protection keys for user account passwords stored in Active Directory
- Protection keys for passwords stored in the registry in the local Security Accounts Manager (SAM) registry key
- Protection keys for Local Security Authority (LSA) secrets

- The protection key for the administrator account password that is used for system recovery startup in safe mode

For all computers in a domain, the secret key is enabled by default and all master keys and protection keys stored on a computer are encrypted with unique 128-bit symmetric random system key.  The system key must be in volatile memory on operation system during system startup to unlock the password protection key.  There are three ways to configure the system key for computers:

1. Use a computer-generated random key as the system key and store it on the local system by using a complex obfuscation algorithm that scatters the system key throughout the registry.  This option allows you to restart the computer without having to enter the system key.  This is the default configuration for the system key.
2. Use a computer-generated random key, but store it on a floppy disk. The system key is not stored anywhere on the local computer, and the floppy disk must be inserted for the system to start.  It is inserted when prompted after Windows 2000 begins the startup sequence, but before it is available for users to log on to the system.
3. Use a password chosen by the administrator to derive the system key. The password is not stored anywhere on the computer.  Windows 2000 prompts the administrator for the password when the system is in the initial startup sequence, but before the system is available for user to log on.

The system key configuration options are available from the system key dialog boxes that appear when you run syskey.  For computers in a domain, you must be a member of the Domain Admin group to run syskey. For stand-alone computers, you must be logged on as the local Administrator to run syskey.  You can configure the system key differently for each computer in the domain.

System key protection is enabled by default in each domain, but you might want to change the default system key option for various computers in a domain.  You also might need to enable system key protection for stand-alone computers.

**Hard Drives**

It is trivial to take the hard drive from one system and read it on another. Hard drives are the goal of any attacker who has physical access to your system.

1. Physically lock the CPU case.  Most desktop and tower cases have locking lugs that you can use to keep an intruder from opening the case.

2. Use a cable-type security lock to keep someone from stealing the whole computer. This is particularly good advice for laptops or small desktops that can easily be hidden inside a backpack or coat.

**Removable Media**

AutoPlay begins reading from a CD-ROM drive as soon as media is inserted in the drive. As a result, the setup file of programs and the sound on audio media starts immediately. This could lead to introduction of viruses and malicious code. **Note:** For more info go to Microsoft Knowledge Base and lookup Q155217. The procedure below works for Windows XP\2000\2003.

Disable Automatically Running CD-ROMs. By default, AutoPlay is disabled on removable drives, such as the floppy disk drive (but not the CD-ROM drive), and on network drives.

• Click Start, click Run, type regedit in the Open box, and then press ENTER.

• Locate and click the following registry key:

**HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CDRom**

• To disable automatically running CD-ROMs, change the Autorun value to 0 (zero). To enable automatically running CD-ROMS, change the Autorun value to 1.

• Restart your computer.

**Additional Information:**

There are two other registry keys that can affect this functionality:

**HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\**

**Policies\Explorer**

**NoDriveTypeAutoRun = 0x00000095**

**-**and-

**HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\**

**Policies\ExplorerNoDriveTypeAutoRun =0x00000095**

**Alternate method using the MMC.**

1. Disable Automatically Running CD-ROMs by snapping in the Group Policy utilizing the MMC.
2. Expand the Local Computer Policy, Computer Configuration, and Administrative Templates folders, till you can click on the System folder.
3. Double click on Disable AutoPlay, and then click on enable. Choose Disable AutoPlay on CD-ROM drives or in the dropdown box choose All Drives.
4. Click on Apply

**NOTE:** By default, AutoPlay is disabled on removable drives, such as the floppy disk drive (but not the CD-ROM drive), and on network drives. If you enable this policy, you can also disable AutoPlay on CD-ROM drives, or disable AutoPlay on all drives. This policy disables AutoPlay on additional types of drives. You cannot use this policy to enable AutoPlay on drives on which it is disabled by default. This policy appears in both the Computer Configuration and User Configuration folders. If these settings conflict, the setting in Computer Configuration takes precedence over the setting in User Configuration. A Media Change Notification (MCN) message from the CD-ROM drive triggers AutoPlay. If the Windows interface does not receive this message, AutoPlay does not operate, regardless of the value of this entry. Entries that suppress the MCN message, such as Autorun and AutoRunAlwaysDisable also disables AutoPlay.

**Lock Workstations**

Here's a great security feature that costs nothing: lock your computer when you're walking away from it. In Windows NT, Windows 2000, Windows XP, or Windows 2003, you only have to quickly hit Ctrl+Alt+Delete, then "k" (the shortcut for the Lock button). Also in Windows XP or Windows 2003, you can quickly hit the windows button and the "L" key to lock your system. Note that a fast-typing attacker can get to your machine and share its disk drives with no passwords in under 10 seconds—but not if the machine's locked!

If workstation consoles are left unattended and not secured, unauthorized personnel could access the workstation and the associated network.

1. Lock your workstation/console whenever a workstation/console is left unattended. Inform your users to do this also.

- For Windows 2000 Press <Ctl>, <alt> <del> simultaneously. The default is "Lock Workstation", then hit Enter or press the k key.

2. For Windows XP/2003 another shortcut is "L, Windows" key.  This will automatically lock your system.

3. For Windows 2000/XP/2003, here is how you can create a shortcut to lock a computer without using the "Ctrl, Alt, Del" keys.

    - Start Windows Explorer.

    - Navigate to \%userprofile%\application data\microsoft\internet explorer\quick launch (for example if you are using the C drive and you are logged on as administrator then go to  C:\documents and settings\administrator\application data\microsoft\internet explorer\quick launch).

    - Right-click in the right-hand pane and select New, Shortcut.

    - Enter "rundll32.exe user32.dll,LockWorkStation" without the quotes and click Next.

    - Name the shortcut "Lock Workstation" and click Finish.

    - To change the icon highlight the following text and select the appropriate icon.

    - Select the icon shortcut you just created.

    - Right click and select properties.

    - Select "Change Icon" in the lower right corner.

    - Select the following text: %SystemRoot%\system32\SHELL32.dll and paste the text in the "File Name" box. Select "OK" and "OK".

    - If you want to place the icon in the System Tray drop and drag the icon to the position desired. Delete the icon on the desktop.

**Screen Saver Passwords**

If a workstation is left unattended and the screen saver is not password protected, unauthorized personnel could access the workstation and the associated network. Make sure all of your workstations have the password protected screensaver feature enabled to prevent an internal threat from taking advantage of an unlocked console. For best results, choose the blank screensaver or logon screensaver.

Implement a Screen Saver Password

- Right click on the desktop background
- Select properties
- Select the "Screen Saver" tab
- Choose a screen saver from the screen saver drop down menu. Make sure you choose one that enables the "password protected"
- Check the password protected box. Your Windows password will now grant you access should the screen saver engage.
- Set the wait time so that the screen will engage in 10 minutes or less. A specified period of 3-5 minutes of no activity is recommended.
- Click on the apply button and close the display properties window.

**Facilities**

Ensure that your facilities meet your security requirements per your security plan.

(Are there appropriate locks installed on the doors?)

Conduct risk assessments which address your physical environment. (Are there false ceilings or floors? Should there be?)

Maintain a proper security environment per requirements ( ie. Tempest, temperature control, black/red separation). (Are you working in a classified environment?)

Make sure you reference your AR 380-5 Department of the Army Information Security Program and any other regulations that refer to your work environment.

Improperly maintained facilities can be a source of service disruption.

- Ensure the following are addressed in you local IA SOP
- Separate black-red communication lines.
- If TEMPEST requirements apply to the system, has TEMPEST testing been accomplished?
- Are TEMPEST test results acceptable or is the physical control zone sufficient.
- Conduct a physical risk assessment.
- Is there adequate power or UPS support available?

- Make sure hardware and software configurations support the security policy.
- Maintain proper temperatures per manufacturer specifications.

**Backup**

The first thing a new or experienced computer user should learn is the importance of backing up. Are you still not backing up your data? You should know this by now: computers can and do fail. The problem is that you usually get no warning before it's too late. This has happened to many people. In extreme cases, it has put companies out of business. Computers are becoming more and more reliable. This creates a false sense of security - we begin to think all our data is safe and secure and will never go away. It's not true - and never will be. If you don't back up your computer system regularly, you are playing Russian roulette with your data. Backups are a necessity, and you are responsible for making backups of your system.  You need to have a thoughtful plan to develop a good backup strategy. Backups are probably the most essential component of any network, but are also one of those things that are done wrong with dreadful regularity. Yet it's not difficult to get your backup strategy right - all it takes is some thought and ongoing motivation.   Here's a four-step process for creating a backup strategy.

1. **Decide what you need to back up.** Do you want to save everything? Only data? What about application settings? Things you've downloaded?
2. **Decide where to back up your data to.** There are plenty of options: a network server, a USB flash, a Zip disk, a (re)writable CD or DVD, a second hard drive, tape, etc. Recommend tape or network server, others may also be a good choice depending on your situation.
3. **Make it easy to back up your data.** Set up your system so that you can back it up with one command. This will take a fair amount of work, but you'll realize its worth when your system crashes. Use a scheduler to schedule automatic backups.
4. **Make daily backups a habit.** The longer the period between backups, the more you have to lose.

Of course all of this depends on your situation, but first you must have a plan.

**Identify the members of the Backup Operators group**

Members of the Backup Operators group can back up and restore files on the computer, regardless of any permissions that protect those files. They can also log on to the computer and shut it down, but they cannot change security settings.

**Caution**

Backing up and restoring data files and system files require permissions to read and write those files. The same default permissions granted to Backup Operators that allow them to back up and restore files also make it possible for them to use the group's permissions for other purposes, such as reading another user's files or installing Trojan horse programs. Group Policy settings can be used to create an environment in which Backup Operators only can run a backup program. Backup Operators should be trusted personnel because they do these have special privileges.

**Identify Systems and data**

Maintain a current and accurate listing of your system's hardware and software**.** Also annotate the type of data you are maintaining, whether it is email, database, or documents.

**Determine the type of backup**

Determine the type of backup that is needed for your system. Windows Backup utility supports five methods of backing up data on your computer or network.

**Normal backup**

A normal backup copies all selected files and marks each file as having been backed up (in other words, the archive attribute is cleared). With normal backups, you need only the most recent copy of the backup file or tape to restore all of the files. You usually perform a normal backup the first time you create a backup set.

**Differential backup**

A differential backup copies files created or changed since the last normal or incremental backup. It does not mark files as having been backed up (in other words, the archive attribute is not cleared). If you are performing a combination of normal and differential backups, restoring files and folders requires that you have the last normal as well as the last differential backup.

**Incremental backup**

An incremental backup backs up only those files created or changed since the last normal or incremental backup. It marks files as having been backed up (in other words, the archive attribute is cleared). If you use a combination of normal and incremental backups, you will need to have the last normal backup set as well as all incremental backup sets in order to restore your data.

**Copy backup**

A copy backup copies all selected files but does not mark each file as having been backed up (in other words, the archive attribute is not cleared). Copying is useful if you want to back up files between normal and incremental backups because copying does not affect these other backup operations.

**Daily backup**

A daily backup copies all selected files that have been modified the day the daily backup is performed. The backed-up files are not marked as having been backed up (in other words, the archive attribute is not cleared).

**Store backed up data off site**

Why store backed up data off site? Imagine your computer catches fire, destroys your office, and melts the backups. Perhaps you should have kept a copy of your Data offsite? It is always a great idea to have your backup stored at an off site incase of a situation like the one above. This off site must be a trusted site. Remember they will have your entire OS and data. When disks are stored safely off-site; this sufficiently reduces the risk of environmental damage (e.g. flood, fire, hurricane), destroying both the primary systems and the off site backups.

**Test the Backup Plan**

You can never rely on a plan if it has not been tested. Plan the test, test the plan. It is your insurance.

**Provide training for those personnel performing backups**

It is very important that all the backup operators are well trained. In case of a disaster, the operator should know where the tapes are stored and the process of recovering the data or backing up the data if needed. It is already stressful that a situation of this magnitude has occurred, so the operator should be well prepared. There should also be a documented process in which the operator has to perform.

**Document all backup requirements and procedure**

Ensure there is a well documented manual with all backup procedures and necessary numbers to contact essential personnel. Make sure that steps have been tested and essential personnel numbers are correct.

**NOTE:** Since backup tapes contain sensitive information from your system, to include user data, and passwords, they become a target for anyone who has physical access to your system.

1. Ensure the following are addressed in you local IA SOP
2. MAKE regular backups.
3. UPDATE your backups whenever you update or change your system.
4. ENSURE that EVERYTHING on your system is addressed in your backup plan.
5. DO NOT reuse a backup tape too many times because it will eventually fail.
6. RESTORE a few files from your backup tapes on a regular basis. This ensures that you have good backup tapes.
7. REBUILD your system from a set of backup tapes to be certain that your backup procedures are complete.
8. KEEP your backup tapes under lock and key.
9. Keep written records of key backup and system configuration information.
10. Store back-up tapes off-site whenever possible.
11. Encrypt back-up tapes whenever possible.

**Uninterruptible Power Supplies**

An Uninterruptible Power Supply is a device that sits between a power supply (e.g. a wall outlet) and a device (e.g. a computer) to prevent undesired features of the power source (outages, sags, surges, bad harmonics, etc.) from the supply from adversely affecting the performance of the device. Unexpected power loss can compromise security and data integrity. For Critical systems you want to have an UPS to protect them, even if you only need an ups to shut down a system safely or to keep a system operating until commercial power resumes.

1. Install Uninterruptible Power Supplies on all critical IT systems.

**Make sure you maintain an updated Emergency Repair Disk (ERD)**
**Windows 2000 only**

The ERD provides the capability to repair or recover a system that can't load
Windows 2000. The ERD provides the capability to repair problems with system
files and the partition boot sector. This situation occurs when the hard disk fails
or when some of the system files are corrupted or accidentally deleted. *System*
*files* are the files Windows 2000 uses to load, configure, and run the operating
system. If some system files are missing or corrupted, you can use the ERD to
repair those files. Try using safe mode or the Recovery console before using an
ERD.

> 1. Repair damaged system with ERD. If a system failure occurs, you can
> start the system using the Windows 2000 Setup CD or the Windows 2000
> Setup floppy disks which can be created by running Makeboot.exe from
> the Boot disk folder on the Windows 2000 Setup CD. Then use the
> Emergency Repair Process to restore core system files.
>
> 2. Re-apply the checklist after a repair to ensure the integrity of the
> security of the system.

**Important ERD Info**

- The ERD allows you to make only basic system repairs, such as to the
  system files, boot sector, and startup environment. The ERD does not
  back up data, programs, or the registry and is not a replacement for
  regular system backups.
- The Windows 2000 ERD, unlike the ERD used with Windows NT, does
  not contain a copy of the registry files. The backup registry files are in the
  folder %SystemRoot%\Repair. However, these files are from the original
  installation of Windows 2000. In the event of a problem, they can be used
  to return your computer to a usable state.
- When you back up system state data, a copy of your registry files is
  placed in the folder %SystemRoot%\Repair\Regback. If your registry files
  become corrupted or are accidentally erased, use the files in this folder to
  repair your registry without performing a full restore of the system state
  data. This method is recommended for advanced users only and can also
  be accomplished by using the Recovery Console commands.

- Because missing or corrupted files are replaced with files from the
  Windows 2000 CD, any changes you made to the system after the original
  installation are lost.
- The ERD must include current configuration information. Make sure that
  you have an ERD for each installation of Windows 2000 on your
  computer, and never use an ERD from another computer.
- To restore your settings from the ERD, the Windows 2000 CD, the
  Windows 2000 Setup disks, and the ERD are required. During the
  restoration process, you can press F1 for more information about your
  options.

**Make sure you maintain an updated Automatic System Recovery (ASR) set
for Windows XP/2003**

ASR is a recovery option that has two parts: ASR backup and ASR restore. You
can access the backup portion through the Automated System Recovery
Preparation Wizard located in Backup or by going to start run and typing the
command ntbackup. The Automated System Recovery Preparation Wizard backs
up the System State data, system services, and all disks associated with the
operating system components. It also creates a floppy disk, which contains
information about the backup, the disk configurations (including basic and
dynamic volumes), and how to accomplish a restore.

You can access the restore part of ASR by pressing F2 when prompted in the
text mode portion of setup. ASR reads the disk configurations from the floppy
disk and restores the entire disk signatures, volumes and partitions on the disks
required to start your computer (at a minimum). (It will attempt to restore all of the
disk configurations, but under some circumstances, it may not be able to). ASR
then installs a simple installation of Windows and automatically starts to restore
from backup using the backup ASR set created by the Automated System
Recovery Preparation Wizard.

**More ASR Info**

System State data is a collection of system-specific data maintained by the
operating system that must be backed up as a unit. It is not a backup of the
entire system. The System State data includes the registry, COM+ Class
Registration database, system files, boot files, and files under Windows File
Protection. For servers, the System State data also includes the Certificate
Services database (if the server is a certificate server). If the server is a domain
controller, the System State data also includes the Active Directory database and
the SYSVOL directory.

**Configuration Management**

Configuration Management is a discipline to ensure that the configuration of a system is known and documented and that changes are controlled and tracked. Configuration Management is rebuilding a system from scratch so that it is not complicated by a lack of documentation. There are instances when Backup tapes/disks are not always enough. Document all hardware and software configurations in a Configuration Management database. Including but not limited to:

- System architecture
- Key nodes and connections identified.
- Software Inventory
- Patches and OS versions information
- BIOS and partitioning information.
- Additional device drivers per requirements.
- Document and mark all cables and connections.

**More Information on SYSKEY**

**To configure system key protection**

1. Type syskey at the command prompt. This brings up the dialog box. After system key protection is enabled, it cannot be disabled.
2. If it is not already selected, click Encryption Enabled, and then click OK. After a reminder that you should create an updated emergency repair disk, you are presented with options for the Account Database Key. The default option is a system-generated password that is stored locally.
3. Select the system key option that you want, and then click OK.
4. Restart the computer. When the system restarts, you might be prompted to enter the system key, depending on the key option you chose. Windows 2000 detects the first use of the system key and generates a new random password encryption key. The password encryption key is protected with the system key, and then all account password information is strongly encrypted.

At subsequent startups:

1. Windows 2000 obtains the system key, either from the locally stored key, the password entry, or insertion of a floppy disk, depending on the options you chose.

2. Windows 2000 uses the system key to decrypt the master protection key.

3. Windows 2000 uses the master protection key to derive the per-user account password encryption key that is then used to decrypt the password information in Active Directory or the local SAM registry key. The syskey command can be used again later to change the system key storage option or to change the password.

4. To change the system key option or password

   - Type syskey at a command prompt to bring up the initial system key dialog box.

   - Click Update.

   - In the Account Database Key dialog box, select a key optin or change the password, and then click OK.

   - Restart the computer.

Changing the system key requires knowledge of, or possession of, the current system key.  If the password-derived system key option is used, syskey does not enforce a minimum password length; however, passwords longer than 12 characters are recommended.  The maximum length is 128 characters.

**Warning**

If the system key password is forgotten or the floppy disk that contains the system key is lost, it might not be possible to start the system. Protect and store the system key safely.  If it is on a floppy disk, make backup copies and store them in a different location.  The only way to recover the system if the system key is lost is by using a repair disk to restore the registry to state prior to enabling system key protection.  This means that you would lose any information or changes which have accrued since then.

System key options can be configured independently on all computers in a domain.  When configured for the system key, each computer has a unique password encryption key and a unique key.  For example, the first domain controller might be configured to use a computer-generated system key stored

on a disk, and secondary domain controllers might each use a different computer-generated system key stored on the local system.  A computer-generated system key stored locally on a primary domain controller is not replicated.

Before enabling the system key when you have a single domain controller, you might want to ensure that a second, complete, updated domain controller is available as a backup system until changes to the first domain controller are complete and verified. Before you change the system key options on a computer, it is recommended that you make a fresh copy of the emergency repair disk for the computer.

**Section 4 – Security Practices**

The three main goals of security are to protect confidentiality, maintain integrity, and assure availability. It should be easy to remember the initials -- "CIA." Loss of one or more of these attributes, can threaten the continued existence of even the largest organization.

**Confidentiality** is assurance that information is shared only among authorized persons or organizations. Confidentiality makes sure private data stays private. Confidentiality can occur when data is not handled in a manner adequate to safeguard the confidentiality of the information concerned. Such disclosure can take place by word of mouth, by printing, copying, e-mailing or creating documents and other data etc.

**Integrity** is assurance that the information is authentic and complete. It ensures that information can be relied upon to be sufficiently accurate for its purpose. The fact the information has not been modified whether intentional or unintentional. The integrity of data is not only whether the data is 'correct', but whether it can be trusted and relied upon.

Example, making copies (say by e-mailing a file) of a sensitive document, threatens both confidentiality and the integrity of the information. Why? Because, by making one or more copies, the data is then at risk of change or modification.

**Availability** is assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.

**Windows Security is based on a simple model of Authentication and Authorization.**

**Authentication**

An essential aspect of security is the ideology of authentication – the ability to prove that someone or something is what it claims to be. Usually, people think of authentication in terms of passwords. Although passwords are frequently used for authentication, there are actually a variety of authentication mechanisms. These mechanisms can generally be categorized as verifying one or more of the following:

- *Something you know*

  This is a traditional password system.

- *Something you have*

This includes mechanisms such as challenge-response lists, one-time pads, smart cards, and so on.

- *Something you are*

  This is the field of biometrics, including techniques such as fingerprint scans, retina scans, voiceprint analysis, and so on.

Something You Know

Authentication that depends on something you know relies on that something's being both hard to guess and secret. In order for you to authenticate reliably, you have to know the secret reliably, too. This isn't as easy as it sounds. Most people are bad at making up and remembering unguessable things and they're worse at keeping secrets. If you use short keys, it's easy to guess them; if you use long keys, it's hard to remember them. If you write them down, you're basically converting to a different type of authentication; now, it's something you have.

Something You Have

Some systems combine these approaches. For example, a smart card that requires the user to enter a personal identification number (PIN) to unlock it is a combination of something you have (the card) and something you know (the PIN). In theory, it is considered a good idea to combine at least two mechanisms (multifactor), because people can steal either one: the thing you have is susceptible to ordinary theft, and the thing you know is compromised by sniffing if it passes over the Internet; but it's rare for somebody to be able to get both at once. Automatic teller machines use this combination; however, ATMs also demonstrate the flaw in the theory: when you are authenticating (standing at the ATM), you reveal what you have (your card) and what you know (your PIN) simultaneously, making yourself vulnerable to a thief who watches you use the machine to capture your PIN, then steals your card as you leave.

Something You Are

There are many types of biometric systems in use or under development today; they test such diverse personal characteristics as your voice, your fingerprint or handprint, your retina, your voice patterns, your signature, and your typing patterns. Biometric systems are extremely attractive, because they get around the problems associated with using things that can be stolen or revealed.  The price tends to be an issue.  Which one is more reliable?

Some alternative biometry technologies are:

- Palm recognition
  Expensive system, not easy to miniaturize

- Iris/Retina recognition
  Not suitable for Navigation, Optical, expensive
- Face recognition
  Expensive system, not easy to miniaturize
- Voice recognition
  Easy to copy voice with tape recorders
- Signature recognition
  Not easy to miniaturize. Not feasible for navigation
- Fingerprint biometrics
  Does not require memorizing codes or passwords.

**Which biometrics?**

Biometrics are about measuring specific characteristics of a person, including:

- Voice
- Handwriting
- fingerprint(s), palm print(s)
- face
- retina of the eye
- iris of the eye.

In an ideal world you want to choose a characteristic of a person that has helpful measuring characteristics such as:

- unlikely to change
- likely to prove unique
- not invasive
- difficult to copy or steal and reproduce.

If you turn these into a matrix you might get the following results. The measuring characteristics are shown as low, medium, high because not every technique is considered precise.

|  | Can't change | Unique | Invasive | Copy |
|---|---|---|---|---|
| **Voice** | L | M | L | H |
| **Handwriting** | M | M | L | M |
| **Fingerprint** | M | M | L | M/H |
| **Face** | L | L | L | H |
| **Retina** | M | H | H | ? |
| **Iris** | H | H | M | ? |

The desired result is to have H, H, L, and L; meaning that they never change, are unique, can be checked without the user feeling they are exposing themselves to any special procedure and are impossible for attackers to copy.

The results of ? for copy are given because at this stage there is little reported evidence of trying to capture and reproduce retina and iris prints, whereas the other techniques listed have been subjected to deliberate attacks with publicized results.

## Authorization

Authorization is based on user rights and the object's permission. The actions an account can perform and the degree to which a user can access information are primarily determined by user rights and permissions. Accounts receive rights and permissions either by having the right or permission assigned directly to the account, or through membership in a group that has been granted the right or permission.

Every application that a user starts runs in that user's security context, not in the application's security context.

Administrators can assign specific rights to group accounts or to individual user accounts. These rights authorize users to perform specific actions, such as logging on to a system or backing up files and directories. User rights are different than permissions: user rights apply to accounts, and permissions are attached to objects (such as printers or folders). Two types of user rights exist:

- Privileges

  A right assigned to an account and specifying allowable actions on the network. An example of a privilege is the right to back up files and directories.

- Logon rights

  A right assigned to an account and specifying the ways in which the account can log on to a system. An example of a logon right is the right to log on to a system locally.

**Improvements in Windows 2000 and Windows 2003**

The Windows 2000 foundation was already a major improvement over Windows NT; technologies such as Kerberos, Encrypted File System (EFS), Public Key Infrastructure (PKI), smart card and biometric support, and especially Active Directory, to name a few, were significant improvements over the basic security capabilities of NT. With Windows Server 2003, Microsoft has reviewed and improved the basic security features included in Windows 2000.

The **Windows 2000 Server** Family provided the following as a major improvement over NT:

- **Group Policy Editor** is a Microsoft Management Console (MMC) snap-in used for configuring and modifying Group Policy settings within Group Policy objects (GPOs).

The Group Policy Object Editor provides administrators with a hierarchical tree structure for configuring Group Policy settings in GPOs. These GPOs can then be linked to sites, domains, and organizational units (OU) containing computer or user objects.

Group Policy Object Editor consists of two main sections: User Configuration, which holds settings that are applied to users (at logon and periodic background refresh), and Computer Configuration, which holds settings that are applied to computers (at startup and periodic background refresh). These sections are further divided into the different types of policies that can be set.

- **IntelliMirror** management is a set of powerful features for change and configuration management.

IntelliMirror combines the advantages of centralized computing with the performance and flexibility of distributed computing.  IntelliMirror ensures that user data, software, and personal settings are available when they move from one computer to another. These settings persist when their computers are connected to the network. Administrators can use Remote Installation Services (RIS) to perform remote installations of the Windows XP operating system. IntelliMirror features are a subset of Group Policy, which in turn requires the Active Directory service.  Most of the IntelliMirror features in Windows XP and Windows Server 2003 family are also available in Windows 2000. You can use IntelliMirror in a network that uses all of these operating systems. However, improvements in the features that were added for Windows XP and

Microsoft® Windows® Server 2003, Standard Edition, provide greater flexibility in administering computers and user accounts in your network.

- **Active Directory**
  Active Directory provides a central place to store information about the users, hardware, applications, and data on the network so users can find what they need.
  It also stores the authorization and authentication information required to ensure that only appropriate users can access each network resource.

- **Multiple Authentication Protocols**
- **Certificate Services**
- **IP Security Extensions (IPSec)**
- **Disk Quota Support**
- **Encrypting File System (EFS)**
- **Kerberos**
- **Layer 2 Tunneling Protocol (L2TP)**
- **Transport Layer Security (TLS) & Secure Socket Layer (SSL)**

**Win2K Security Issues**
- More complex then other versions of Windows
- 3rd party software incorporated into OS
    - IPSec, Kerberos

**Win2K Features or Issues**
- Automatic Log-on Support
- Indexing Service
- Single Sign-on
    - Directory information can be accessed by various operating systems
    - Allows users the ability to access files, printers, web services with one sign-on
- Kerberos Support
    - MS version of Kerberos
    - Win2K networks only

**The Windows Server 2003 Family provides the following**:

- A more secure platform
- The best platform for your public key infrastructure
- Secure extension of your business to the Internet

**Windows 2003 Security Features**
- Internet Connection Firewall
- Secure IAS/RADIUS Server
- Secure Wireless and Ethernet LANs

- Software Restriction Policies
- Security Improvements for Servers on Ethernet and Wireless LANs
- Increased Web Server Security
- Encrypting the Offline Files Database
- FIPS-compliant, Kernel-mode, Crypto Module
- New Digest Security Package
- System Security Improvements
- Credential Manager

## Other Window 2003 improvements

## Encrypting File System improvements

Encrypting File System (EFS) has been improved in several ways. Stronger
encryption algorithms are available with larger keys. Multiple users can be
authorized to share encrypted files. Offline files can be encrypted through EFS,
so that you can protect locally cached documents

## Software restriction policies

With software restriction policies, you can protect your computer environment
from untrusted code by identifying and specifying which applications are allowed
to run.

## Internet Protocol security monitoring improvements

Internet Protocol security (IPSec) monitoring improvements include a Microsoft
Management Console (MMC) snap-in that provides detailed information about
IPSec policy.  This feature replaces the Ipsecmon.exe monitor program in
Windows 2000.

## Trusts

A trust is a relationship established between domains that enable users in one
domain to be authenticated by a domain controller in the other domain. Trust
relationships in Windows NT are different than in Windows 2000 and Windows
Server 2003 operating systems.

## Trusts in Windows NT

In Windows NT 4.0 and earlier, trusts are limited to two domains and the trust
relationship is one-way and nontransitive. Nontransitive is a trust relationship in a
multiple-domain environment that is restricted to just two domains. For example,
if domain A has a nontransitive trust with domain B, and domain B trusts domain
C, then there is no trust relationship between domain A and domain C.
Nontransitive trusts can be one-way or two-way. For example, domain A trusts

domain B, and domain B does not trust domain A. One-way trusts are often used to enable authenticated access to resource domains.  In the following figure, the nontransitive is shown by the straight arrow pointing to the trusted domain, the curved arrow shows the direction of access.
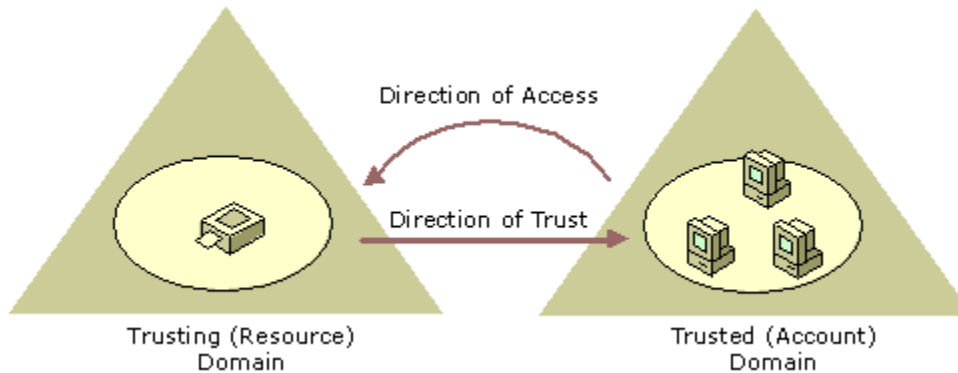


## Trusts in Windows Server 2003 and Windows 2000 server operating systems

All trusts in a Windows 2000 and Windows Server 2003 forest are transitive, two-way trusts. Transitive trust is a trust relationship that flows throughout a set of domains, such as a domain tree, and forms a relationship between a domain and all domains that trust that domain. For example, if domain A has a transitive trust with domain B, and domain B trusts domain C, then domain A trusts domain C. Transitive trusts can be one-way or two-way, and they are required for Kerberos-based authentication and Active Directory replication. A two-way trust is a trust relationship between two domains in which both domains trust each other. For example, domain A trusts domain B, and domain B trusts domain A. All parent-child trusts are two-way. Therefore, both domains in a trust relationship are trusted. As shown in the following figure, this means that if Domain A trusts Domain B and Domain B trusts Domain C, then users from Domain C can access resources in Domain A (when assigned the proper permissions). Only members of the Domain Admins group can manage trust relationships.
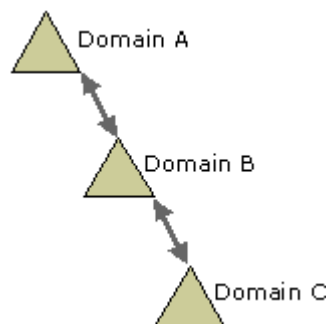
**Registry**
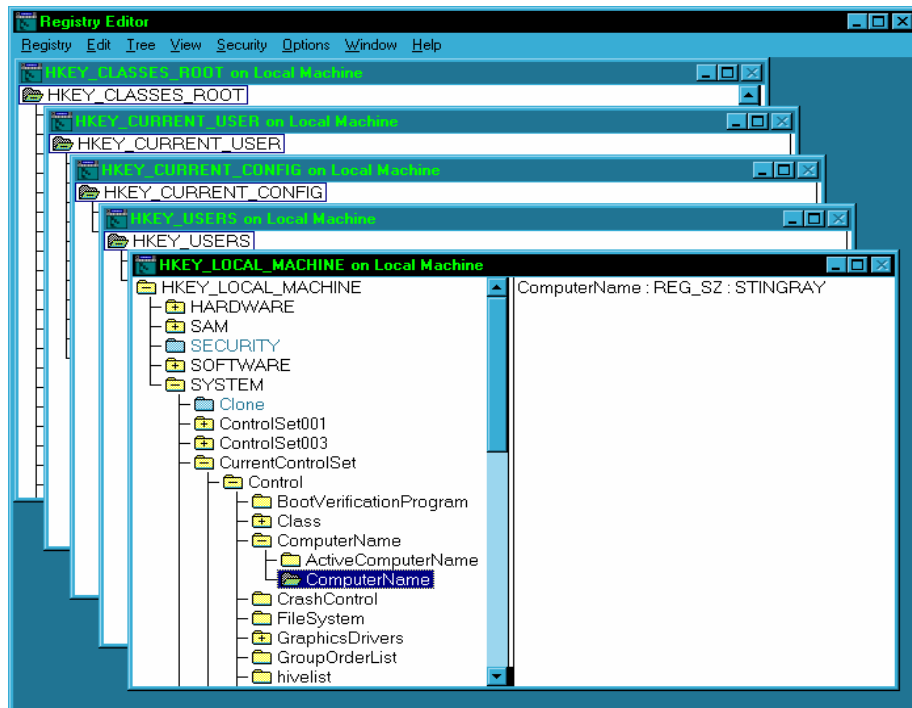


## Overview of the Windows Registry

The Windows registry is a centralized hierarchical database that stores the values of variables and the applications and services that run on Windows. The operating system and other programs also use the registry to store data about users and about the current configuration of the system and its components. Because the registry is available whenever the system is running, programs that start and stop can keep persistent data in the registry.

The registry consists of nested containers known as subtrees, keys, and subkeys, which are like folders. The registry is utilized to impose order on the configuration.  It contains hardware configuration data, application configuration data, service and device driver configuration data, and network protocol and adapter card settings.  To maintain compatibility with older versions of application programs .ini files may still be utilized for configuration files and scattered throughout the disk.

## Editing the Registry

Most users never need to edit the registry. You can configure most system services by using the programs provided with Windows:

- Computer Management
- Control Panel

- Group Policy
- Administrative tools that install with optional services (such as WINS Manager and Internet Service Manager).

**Using the Registry Editor**

If you need to view the registry or to change a value that can be changed only in the registry directly, use Regedit.exe, the registry editor installed with Windows Server 2003. An alternative registry editor, Regedt32.exe, which is included in Windows 2000 and earlier, is not included in Windows Server 2003, although many of its functions appear in the Windows Server 2003 version of Regedit.exe.

**HKEY_CURRENT_CONFIG** (HKCC)

The HKEY_CURRENT_CONFIG (HKCC) subtree stores configuration data for the current hardware profile.

This subtree does not contain any data. It just stores a pointer to the content of the Current subkey in the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles subkey. The content of the Current subkey appears in HKEY_CURRENT_CONFIG, and it can be viewed and changed in either location. This subtree provides easier access to the data.

**HKEY_CLASSES_ROOT** (HKCR)

The HKEY_CLASSES_ROOT subtree contains two types of data:

1.  Data that associates file types with programs. The file type subkeys in HKEY_CLASSES_ROOT have the same name as the file name extension for the file type, such as .exe. File type associations are stored in the registry, but you should use Windows Explorer to change them. In Windows Explorer, from the **Tools** menu, click **Folder Options**, and then click the **File Types** tab.

2.  Configuration data for COM objects, Visual Basic programs, or other automation. The configuration subkeys use either the program IDs (such as for COM, Visual Basic, automation, and scripting) or parent keys for other classes of information (such as for CLSID, Interface, TypeLib, AppId, and so on).

**HKEY_CURRENT_USER**  (HKCU)

The HKEY_CURRENT_USER subtree contains the user profile for the user who is currently logged on to the computer. The user profile includes environment variables, personal program groups, desktop settings, network connections, printers, and application preferences. The HKEY_CURRENT_USER subtree

does not contain any data. It just stores a pointer to the content of the
HKEY_USERS\\*Security ID (SID) of current user* subkey. Therefore, the content
of that subkey also appears in HKEY_CURRENT_USER, and it can be viewed
and changed in either location. The HKEY_CURRENT_USER subtree just
provides easier access to the data.

A new HKEY_CURRENT_USER subtree is created each time a user logs on.
The data for the subtree comes from the profile of the current user. If no profile is
available, then the subtree is built from the user profile settings established for a
default user, which are stored in *System drive*\\Documents and Settings\\Default
User (WINNT)\\Ntuser.dat.

 **HKEY_USERS** contains information on all the active, loaded user profiles.  It
includes the default user profile and the HKEY_CURRENT_USER subtree key,
which is a child of HKEY_USERS.

**HKEY_LOCAL_MACHINE** (HKLM)

The HKEY_LOCAL_MACHINE subtree contains information about the local
computer system, including hardware and operating system data, such as bus
type, system memory, device drivers, and startup control parameters.

**Hive**
A hive consists of a particular set of Registry keys, subkeys, and values.  Each
hive is rooted at the top to the registry hierarchy and is stored in a separate file.

**Registry Hives**
The Registry Hives map directly to operating system files. The term HIVE is a MS
term.  A hive is a file in which data from specific registry subtrees are stored.
Hives differ from other groups of keys in that they are permanent components of
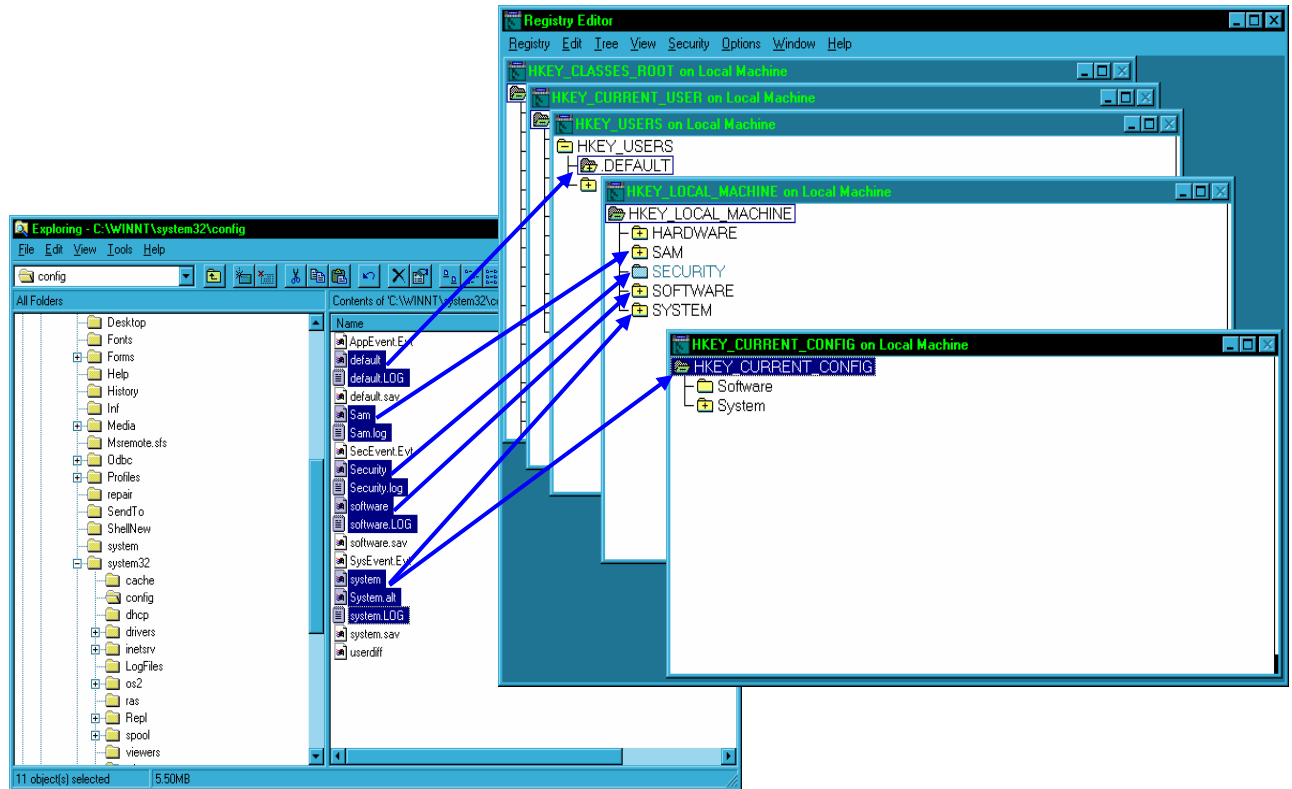
the registry; they are not created dynamically when the system starts nor are they deleted when it is shutdown (e.g. HKEY_LOCAL_MACHINE\Hardware, which is built dynamically when Windows NT starts, is not considered a hive).

The 6 hives and their associated registry location are as follows:

| | |
|---|---|
| SAM | HKEY_LOCAL_MACHINE\SAM |
| Security | HKEY_LOCAL_MACHINE\Security |
| Software | HKEY_LOCAL_MACHINE\Software |
| System | HKEY_LOCAL_MACHINE\system and HKEY_CURRENT_CONFIG |
| Ntuser.dat | HKEY_CURRENT_USER |
| Default | HKEY_USERS\.DEFAUKT |

All hive data except HKEY_CURRENT_USER are stored in individual files in the %SystemRoot%\system32\config directory along with their associated .LOG file. The HKEY_CURRENT_USER support files are stored in the user subdirectories of %SystemRoot%\Profiles.  The Ntuser.dat file in each profile subdirectory stores user profile and policy information, and the Ntuser.dat.log file tracks changes to Ntuser.dat.

These files are important and should be secured.

When you start assigning permissions to or editing a registry key, you must be very cautious. Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer. You must have appropriate permissions to make changes to a registry key. To maintain security when making changes to a registry key for which you need administrative credentials, it is recommended that you log in as a member of the Users group and run Regedit/Regedt32 as an administrator by right-clicking the Regedit/Regedt32 icon, clicking Run as, and clicking an account in the local Administrators group.

## Section 5 – Added Security Measures

**File Format Recommendations**

It is recommended that you use NTFS 5.0 partitions and avoid whenever possible the use of FAT16 or Fat32. It is best to format the system to NTFS, but if it is not possible, use the convert utility to convert partition to NTFS.

- This set Access Control Lists (ACLs) of the converted partition to Everyone: Full Control For Windows 2000 (Note: This is a bad thing, you do not want everyone to have full control). In Windows 2003 by default Everyone is limited to Read and other special permissions.

- Fat16 or Fat32 do not provide file/folder security support, encryption and disk quotas.

Make sure that all partitions on your server are formatted using NTFS. If necessary, use the convert utility to non-destructively convert your FAT partitions to NTFS.

**Use Dynamic Disks**

Dynamic disks provide features that basic disks do not, such as the ability to create volumes that span multiple disks (spanned and striped volumes), and the ability to create fault tolerant volumes (mirrored and RAID-5 volumes). All volumes on dynamic disks are known as dynamic volumes.

Dynamic Disks are not recognized by other OS, except Linux with special tools are able to detect dynamic disks. With these special tools Linux is able to keep searching past the first 1 MB of space on the hard drive, not like other Operating Systems. Disk Configuration data is stored in the last 1 MB of space on Hard drive.  On a basic disk the data configuration data is stored in the first 1 MB of space on hard drive.

**Note:**  Do not convert basic disks to dynamic disks if they contain multiple installations of Windows 2000, Windows XP Professional, or the Windows Server 2003 family of operating systems. After the conversion, it is unlikely that you will be able to start the computer using that operating system. Dynamic disks are not supported on portable computers or Microsoft Windows XP Home Edition. DOS Volumes only allow share file/directory security.  DOS partition

could provide a door way to the rest of the system.  A user who has physical access to the machine could boot into DOS and use ntfsdos.exe to gain access to critical areas of the OS.

| Key Issues about Dynamic Disks |
| --- |
| Not recognized by other OS (except Linux w/special tools) |
| Defeats the NTFS DOS threat. |
| Disk configuration data is stored in last 1 MB of space of HD |
| Changes are not recorded in partition table |

## NTFS Alternate Data Streams (ADS)

- Developed by Microsoft for compatibility with Apples' Macintosh Hierarchical File System (HFS).

- Why would Microsoft do that?  They developed a version of Microsoft Office for Macintosh and needed the ability to share information between HFS and NTFS.

- Malicious users take advantage of this by storing a virus or Trojan on your system.  Users can abuse this by hiding graphics or data behind text files, etc.

- How to create an Alternate Data Stream:  The syntax used to create the Stream is straightforward.  An ADS associated with the file normal.txt, simply separate the default stream name from the ADS name with a colon. (normal.txt:hidden.txt)

- What Can Be hidden using ADS?   Many things can be hidden using ADS, various types of Data and many types of executables (for example programs, games, root kits, hacker tools)

- What type can ADS have?   They can be compressed or encrypted.

| Key issues about NTFS Data Streams |
| --- |
| Streams are only visible to specialized software. |
| Public awareness of streams is very low. |
| Streams can attach themselves to directories as well as files. |
| Disk space used by Streams are not reported by programs such as Windows Explorer or commands such as 'DIR' |
| Streams can be executed. |
| Executed streams do not have their filenames displayed correctly in Windows Task Manager. |

This relatively unknown compatibility feature of NTFS, Alternate Data Streams (ADS) provides hackers with a method of hiding root kits, hacker tools, data, photos or all types of executables on a breached system and allows them to be executed without being detected by the systems administrator.

Alternate Data Streams are relatively easy to make and require little or no skill on the part of the hacker. Common DOS commands like "type" are used to create an ADS. These commands are used in conjunction with a redirect [>] and colon [:] to fork one file into another.

ADSs are a feature of the NTFS file system intended to provide compatibility with HFS, which may still be necessary for compatibility. However, the lack of visibility of this "feature" poses a significant risk for administrators. There has already been one virus released that employed ADSs.  As the release of malware and incidents of cybercrime increase, the malicious use of ADSs will likely increase as well.

The solution is not to stop using the NTFS file system, as the benefits in security and reliability are too great. This "feature" has remained part of the file system since NT 3.1. Given the circumstances, a far more prudent solution would have been to include support for HFS files in the File and Print Services for the Macintosh, rather than the file system. As it is, administrators should make judicious use of discretionary access control lists (DACLs) on files and directories, and regularly scan their critical systems using utilities such as lads.exe or streams.exe. Microsoft should be adding the ability to detect and view ADSs to Windows Explorer and the command interpreter.

Due to the manner in which the command line is parsed streams are not displayed in file management utilities.   Some of the security considerations with respect to streams are
- data will be added to user's quota
- most virus scanners do not attempt to discover and scan streams
- fragmentation could hinder performance
- used as a covert channel
- survive copy operations between computers supporting NTFS and backup operations


If you have Windows 2000, XP or 2003 and use NTFS (which we all should), test your system, scan your hard drives looking for suspicious streams. Software needed for scanning your system is streams.exe from SysInternals (http://www.sysinternals.com/ntw2k/source/misc.shtml)
Or List Alternate Data Streams  lads.exe from Frank Hayne Software (http://www.heysoft.de/Frames/f_sw_la_en.htm).

**Permissions**

Permissions define the type of access granted to a user or group for an object or object property. Permissions are applied to any secured objects such as files, Active Directory objects, or registry objects. Permissions can be granted to any user, group, or computer. It is a good practice to assign to groups.

You can assign permissions for objects to:

- Groups, users, and special identities in the domain.

- Groups and users in that domain and any trusted domains.

- Local groups and users on the computer where the object resides.

The permissions attached to an object depend on the type of object. For example, the permissions that can be attached to a file are different from those that can be attached to a registry key. Some permissions are common to most types of objects. These common permissions are:

- Read permissions

- Modify permissions

- Change owner

- Delete

When you set up permissions, you specify the level of access for groups and users. For example, you can let one user read the contents of a file, let another user make changes to the file, and prevent all other users from accessing the file. You can set similar permissions on printers so that certain users can configure the printer and other users can only print from it.

If you need to change the permissions on an individual object, you can simply start the appropriate tool and change the properties for that object. For example, to change the permissions on a file, you can run Windows Explorer, right-click the file name, and click Properties. Click on the security tab, there you will see name and permission.

Ownership of objects

An owner is assigned to an object when that object is created. By default, the owner is the creator of the object. No matter what permissions are set on an object, the owner of the object can always change the permissions on an object.

## Inheritance of permissions

Inheritance allows administrators to easily assign and manage permissions. This feature automatically causes objects within a container to inherit all the inheritable permissions of that container. For example, the files within a folder, when created, inherit the permissions of the folder. Only permissions marked to be inherited will be inherited.

Authorization is the process of verifying that the client is allowed to connect to the server and perform necessary jobs.

Each type of object is controlled by an object manager. There is a different object manager for each type of object. The object types, their object managers, and the tools you use to manage these objects are as follows:

## File and Folder

Folder permissions include Full Control, Modify, Read & Execute, List Folder Contents, Read, and Write.  Where file permissions include Full Control, Modify, Read & Execute, Read and Write (not List Folder Contents). There are also special permissions associated with these permissions.

## File and folder special permissions

| Special Permissions | Full Control | Modify | Read & Execute | List Folder Contents(folders only) | Read | Write |
|---|---|---|---|---|---|---|
| Traverse Folder/Execute File | x | x | x | x | | |
| List Folder/Read Data | x | x | x | x | x | |
| Read Attributes | x | x | x | x | x | |
| Read Extended Attributes | x | x | x | x | x | |
| Create Files/Write Data | x | x | | | | x |
| Create Folders/Append Data | x | x | | | | x |
| Write Attributes | x | x | | | | x |
| Write Extended Attributes | x | x | | | | x |
| Delete Subfolders | x | | | | | |

and Files

| | | | | | | |
|---|---|---|---|---|---|---|
| Delete | x | x | | | | |
| Read Permissions | x | x | x | x | x | x |
| Change Permissions | x | | | | | |
| Take Ownership | x | | | | | |
| Synchronize | x | x | x | x | x | x |

To set, view, change, or remove permissions on files and folders

- Open Windows Explorer.
- Right-click the file or folder for which you want to set permissions, click Properties, and then click the Security tab.
- To set permissions for a group or user that does not appear in the Group or user names box, click Add. Type the name of the group or user you want to set permissions for and then click OK.
- To change or remove permissions from an existing group or user, click the name of the group or user.
- To allow or deny a permission, in the Permissions for *User or Group* box, select the Allow or Deny check box.
- To remove the group or user from the Group or user names box, click Remove.
- To open Windows Explorer, click Start, point to All Programs, point to Accessories, and then click Windows Explorer.

In the Windows Server 2003 family, the Everyone group no longer includes Anonymous Logon.

You can only set file and folder permissions on drives formatted to use NTFS.

To change permissions, you must be the owner or have been granted permission to do so by the owner.

Groups or users that are granted Full Control for a folder can delete files and subfolders within that folder, regardless of the permissions that protect the files and subfolders.

If the check boxes under Permissions for *User or Group* are shaded or if the Remove button is unavailable, then the file or folder has inherited permissions from the parent folder.

**Assigning printer permissions**

When a printer is installed on a network, default printer permissions are assigned that allow all users to print, and allow select groups to manage the printer, the

documents sent to it, or both. Because the printer is available to all users on the network, you might want to limit access for some users by assigning specific printer permissions. For example, you could give all nonadministrative users in a department the Print permission and give all managers the Print and Manage Documents permissions. In this way, all users and managers can print documents, but managers can also change the print status of any document sent to the printer.

Windows provides three levels of printing security permissions: Print, Manage Printers, and Manage Documents. When multiple permissions are assigned to a group of users, the least restrictive permissions apply.

**To assign permissions to a registry key (Windows 2000)**

- Open Registry Editor. (Start – Run – Regedt32)
- Click the key to which you want to assign permissions.
- On the Security menu, click Permissions.

To grant the user permission to read the key contents, but not save any changes made to the file, under Permissions for name, for Read, select the Allow check box.

To grant the user permission to open, edit, and take ownership of the selected key, under Permissions for name, for Full Control, select the Allow check box.

To grant the user special permission in the selected key, click Advanced.

**To assign permissions to a registry key (Windows 2003)**

- Open Registry Editor. (Start – Run - Regedit or Regedt32)
- Click the key to which you want to assign permissions.
- On the Edit menu, click Permissions.
- Assign an access level to the selected key as follows:

To grant the user permission to read the key contents, but not save any changes made to the file, under Permissions for name, for Read, select the Allow check box.

To grant the user permission to open, edit, and take ownership of the selected key, under Permissions for name, for Full Control, select the Allow check box.

To grant the user special permission in the selected key, click Advanced.

**Share permissions**

A shared resource provides access to applications, data, or a user's personal data. You can assign or deny permissions for each shared resource. You can control access to shared resources with a variety of methods. You can use share permissions, which are simple to apply and manage. Or, you can use access control on the NTFS file system, which provides more detailed control of the shared resource and its contents. You can also use a combination of these methods. If you use a combination of these methods, the more restrictive permission always applies. For example, if the share permission is set to Everyone = Read (which is the default for Windows 2003), and the NTFS permission allows users to make changes to a shared file, the share permission applies, and the user is not allowed to change the file. The default with Windows 2000 is Everyone = Full Control. This is a security hazard.

**Services permissions**

There are two types of permissions that apply to services: service account permissions and service permissions. Service account permissions refer to the user rights and credentials that are granted to the service through the logon account. There are two types of user rights: privileges and logon rights. An example of a privilege is the right to shut down the system. An example of a logon right is the right to log on to a computer locally. The entire listing of both privileges and logon rights are shown above in the section on user rights. Both types are assigned by administrators to individual users or groups as part of the security settings for the computer. Examples of credentials are user names and passwords, smart cards, and certificates. Service permissions refer to the permissions that are required to configure a service.

**Service account permissions**

A service must log on to an account to access resources and objects on the operating system. Most services are not designed to have their default logon account changed. Changing the default account will probably cause the service to fail. If you select an account that does not have permission to log on as a service, the Services snap-in automatically grants that account the user rights that are required to log on as a service on the computer that you are managing. However, this does not guarantee that the service will start.

**Access Control List  (ACL)**
ACL is a list of security protections that applies to an object. (An object can be a file, process, event, or anything else having a security descriptor.) An entry in an access control list (ACL) is an access control entry (ACE). There are two types of access control list, discretionary and system.

**Discretionary access control list (DACL)**
DACL is an access control list (ACL) that is controlled by the owner of an object and that specifies the access particular users or groups can have to the object. DACL identifies the trustees that are allowed or denied access to a securable object. When a process tries to access a securable object, the system checks the acess control entries ACE's in the object's DACL to determine whether to grant access to it. If the object does not have a DACL, the system grants full access to everyone. If the object's DACL has no ACEs, the system denies all attempts to access the object because the DACL does not allow any access rights. The system checks the ACEs in sequence until it finds one or more ACEs that allow all the requested access rights, or until any of the requested access rights are denied.

**System Access Control List (SACL)**
SACL is an ACL that controls the generation of audit messages for attempts to access a securable object. The ability to get or set an object's SACL is controlled by a privilege typically held only by system administrators.


**Service Packs/Hotfixes/Patches**

Army personnel are reminded that they do not have to wait for an Information Assurance Vulnerability Management (IAVM) to patch their systems IAW AR 25-2 Chapter 3-3a (6) all System/Network Administrators are required to ensure secure configurations to include all pertinent patches and fixes by routinely reviewing vendor sites, bulletins, and notifications and proactively updating systems with fixes, patches, definitions, service packs, or implementation of vulnerability mitigation strategies with Information Assurance Manager (IAM) or Information Assurance Program Manager (IAPM) approval.

**Best Practices**

These apply to all updates regardless of whether they are service packs, hotfixes or security patches. The generic items listed below are recommended steps that need to be performed across all updates. In addition, there are specific best practices for each type of update, and these are listed under each update.

**Use a change control process**

A good change control procedure has an identified owner, a path for customer input, an audit trail for any changes, a clear announcement and review period, testing procedures, and a well-understood back-out plan. Change control will manage the process from start to finish. If your current procedure is lacking any

of the above, please reconsider carefully before using it for deployment of updates.

**Read all related documentation**

Before applying any service pack, hotfix or security patch, all relevant documentation should be read and reviewed. The review process is critical as it mitigates the risk of a single person missing critical and relevant points when evaluating the update. Reading all associated documentation is the first step in assessing whether: The update is relevant, and will resolve an existing issue. Its adoption won't cause other issues resulting in a compromise of the production system. There are dependencies relating to the update, (i.e. certain features being enabled or disabled for the update to be effective.)

Potential issues will arise from the sequencing of the update, as specific instructions may state or recommend a sequence of events or updates to occur before the service pack, hotfix or security patch is applied.

Documentation released with the updates is usually in the form of web pages, attached Word documents and README.TXT files. These should be printed off and attached to change control procedures as supporting documentation.

**Testing**

The prior points really assist in giving you a feel (before installing) for the potential impact, however, testing allows for the "test driving" and eventual signing off of the update. Service packs and hotfixes must be tested on a representative non-production environment prior to being deployed to production. This will help to gauge the impact of such changes.

**Plan to uninstall**

Where possible, service packs, hot fixes and security patches must be installed such that they can be uninstalled, if required. Historically, service packs have allowed for uninstalling, so verify there is enough free hard disk space to create the uninstall folder.

**Consistency across Domain Controllers**

Service packs, hot fixes and security patch levels must be consistent on all Domain Controllers (DCs). Inconsistent update levels across DCs can lead to DC-to-DC synchronization and replication related problems. It is extremely difficult to trap errors caused by DCs being out of sync, so it's critical that consistency is maintained. Where it is practical, Member Servers should also be updated with the same service packs and hot fixes as the Domain Controllers.

**Have a working Backup and schedule production downtime**

Server outages should be scheduled and a complete set of backup tapes and emergency repair disks should available, in case a restoration is required. Make sure that you have a working backup of your system. The only supported method of restoring your server to a previous working installation is from a backup.

**Always have a back-out plan**

A back-out plan will allow the system and enterprise to return to their original state, prior to the failed implementation. It is important that these procedures are clear, and that contingency management has tested them, because in the worst case a faulty implementation can make it necessary to activate contingency options. Enterprises may need to exercise their back-out plan in the event of the update not having an uninstall process or the uninstall process failing. The back-out plan can be as simple as restoring from tape, or may involve many lengthy manual procedures.

**Forewarn helpdesk and key user groups**

You need to notify helpdesk staff and support agencies (such as Microsoft Product Support Service - PSS) of the pending changes so they may be ready for arising issues or outages.

In order to minimize the user impact, it is also a good idea to prepare key user group of proposed updates, this will assist in managing user expectations

**Don't get more than 2 service packs behind**

Schedule periodic service pack upgrades as part of your operations maintenance and try never to be more than two service packs behind

**Target non-critical servers first**

If all tests in the lab environment are successful, start deploying on non-critical servers first, if possible, and then move to the primary servers once the service pack has been in production for 10-14 days.

To verify the most-current service pack for Windows is installed.
- From the menu bar click "Start" and then "Run".
- Type "winver.exe" in the dialog box and click OK.
  (You should see a dialog box that displays the OS information and any service packs)

**For Windows 2000**
**POSIX OS/2 Support**

Ensure that support for POSIX and OS/2 is removed from the 2000 Server.
Vulnerabilities exist that could be exploited if not removed. OS/2 and POSIX
subsystems are actually mapped to calls in the Win32 subsystem where the
actual functionality is implemented. This can allow programs written for these
subsystems to run at root. For Windows 2003, if POSIX and OS/2 are needed
you will have to install them.

**POSIX  Subsystem File Components (to remove it from Windows 2000)**

- Select the "Search" button from the Tools bar.
- Enter the following name in the "Search for files and
 folders named" field: **POSIX PSX.**
- Click on the "Search Now" button.
- If the search indicates that the files "POSIX.EXE," "PSXSS.EXE" or
  "PSXDLL.DLL" are present then the option is considered to be on.
- Remove the above listed items.

**OS/2 Subsystem File Components (to remove it from Windows 2000)**
- Select the "Search" button from the Tools bar.
- Enter the following name in the "Search for files and folders named"
  field: **OS2**
- Click on the "Search Now" button.
- If the search indicates that the files "OS2SS.EXE," "OS2.EXE" or
  "OS2SRV.EXE" exist, or the directory "OS2" exists, then the option is
  considered to be on.
- Remove the above listed items.
- OS2 files should also be removed from the \dllcache directory,
  otherwise Windows 2000 will restore them. In rare instances some mail
  servers require the OS/2 modules to function properly.  If these
  exceptions are not documented, you should remove all of the above
  files.

**For Windows 2003**

**POSIX support**

The Portable Operating System for UNIX (POSIX) subsystem is not included with
Windows XP or with Windows Server 2003. The POSIX subsystem has been
replaced with a more UNIX-like environment that is named Windows Services for
UNIX. Windows Services for UNIX is a superset of the original POSIX subsystem
and provides greater functionality for UNIX programs. Windows Services for
UNIX requires Windows XP Professional Service Pack 1 (SP1) or later.

**OS/2 support**

The OS/2 subsystem is not included with Windows XP or with Windows Server 2003. An alternative solution for OS/2 programs is Microsoft Virtual PC 2004. Virtual PC 2004 supports most OS/2 programs including OS/2 programs that have a graphical user interface (GUI).

**Encrypting File System (EFS)**

The Encrypting File System provides the core file encryption technology used to store encrypted files on NTFS file system volumes. Once you encrypt a file or folder, you work with the encrypted file or folder just as you do with any other files and folders. Encryption is transparent to the user that encrypted the file. This means that you do not have to decrypt the encrypted file before you can use it. You can open and change the file as you normally do. However, an intruder who tries to access your encrypted files or folders will be prevented from doing so. An intruder receives an access denied message if the intruder tries to open, copy, move, or rename your encrypted file or folder.

You encrypt or decrypt a folder or file by setting the encryption property for folders and files just as you set any other attribute such as read-only, compressed, or hidden. If you encrypt a folder, all files and subfolders created in the encrypted folder are automatically encrypted. It is recommended that you encrypt at the folder level.

You can also encrypt or decrypt a file or folder using the command-line function **cipher**. Using EFS helps to keep your documents safe from intruders who might gain unauthorized physical access to your sensitive stored data (by stealing your laptop or Zip disk).

Encrypting File System
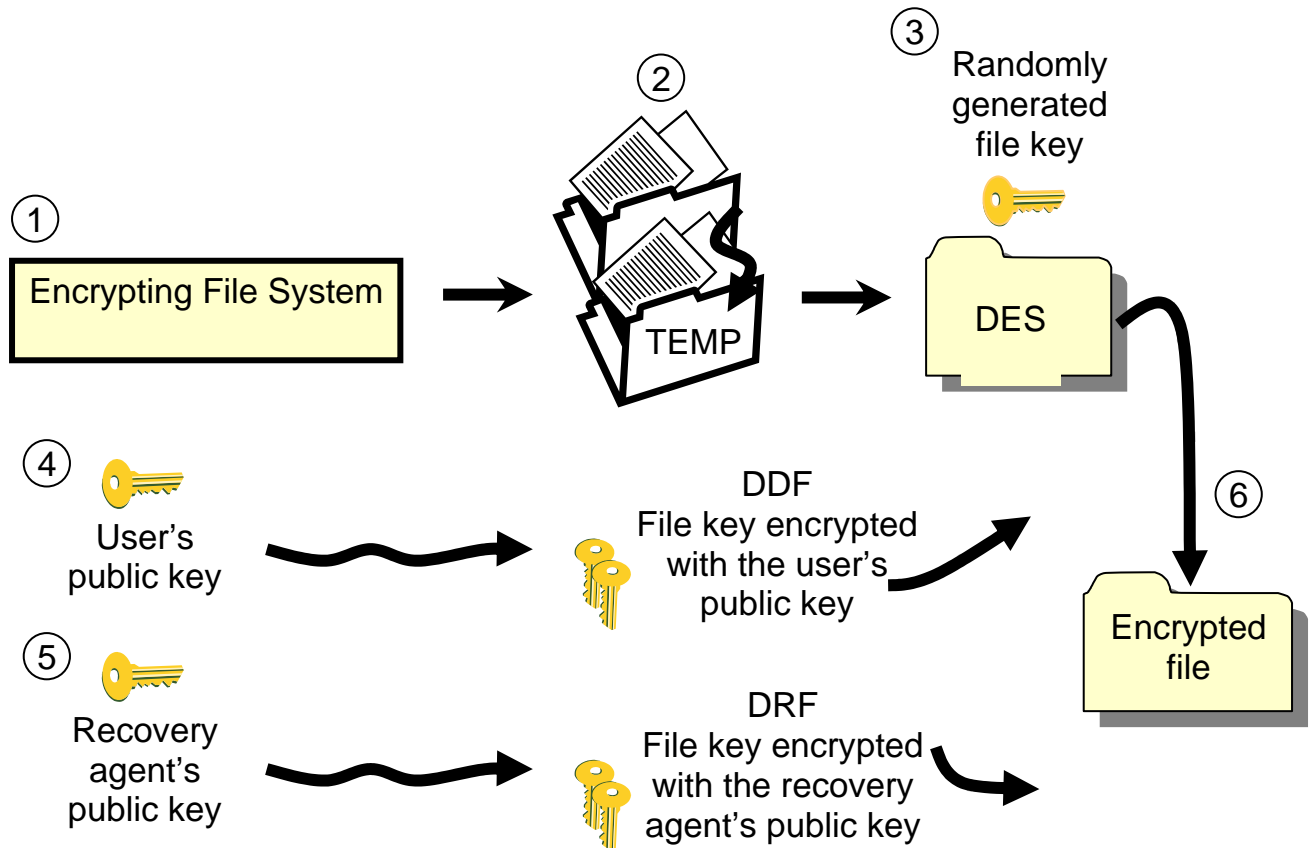


When a user encrypts a file in EFS, the following process occurs:
1. The EFS service opens the file for exclusive access.
2. All data streams in the file are copied to a temporary file.
3. A file key is randomly generated and used to encrypt the file according to the DES encryption scheme.
4. A Data Decryption Field (DDF) is created that contains the file key, which is encrypted with the user's public key.
5. A Data Recovery Field (DRF) is created that contains the file key, this time encrypted with the recovery agent's public key. The recovery agent's public key is obtained from the Encrypted Data Recovery Policy (EDRP).
6. The EFS service writes the encrypted data, along with the DDF and DRF, back to the file.
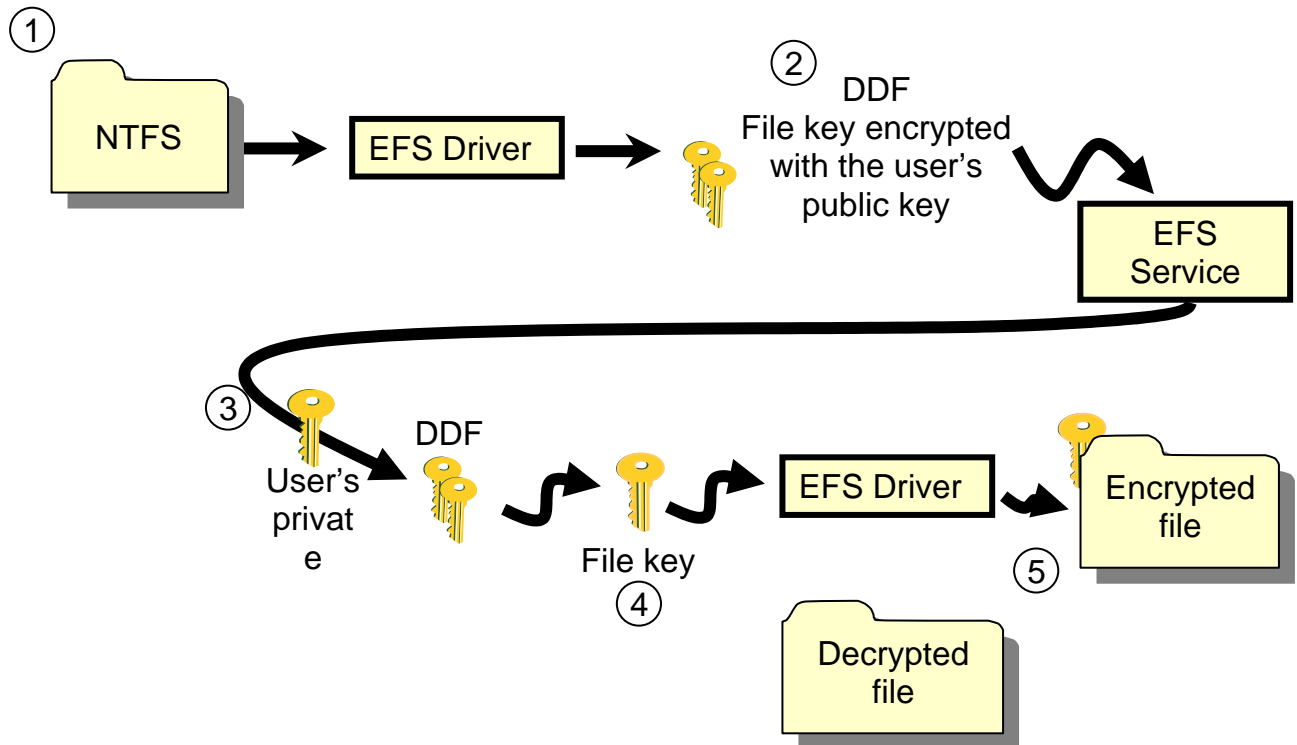
When a file is decrypted in EFS, the following process occurs:
1. When an application accesses an encrypted file, NTFS recognizes the file as encrypted and sends a request to the EFS driver.
2. The EFS driver retrieves the DDF and passes it to the EFS service.
3. The EFS service decrypts the DDF with the user's private key to obtain the file key.
4. The EFS service passes the file key back to the EFS driver.
5. The EFS driver uses the file key to decrypt the file.
6. The EFS driver returns the decrypted data to NTFS, which then completes the file request, and sends the data to the requesting application.

**Working with encrypted files**

When you work with encrypted files and folders, keep in mind the following information and recommendations.

**Important EFS Information**

- Only files and folders on NTFS volumes can be encrypted. NTFS is required.

- You cannot encrypt files or folders that are compressed. First you must uncompress the file or folder, and then you can encrypt it. On a compressed volume, uncompress folders you want to encrypt.

- Only the user who encrypted the file (and the data recovery agent) can open it.

- You cannot share encrypted files with Windows 2000. You can share encrypted files in Windows XP/2003.

- Encrypted files will be decrypted if you copy or move the file to a volume that is not an NTFS volume. Encrypted files moved across the network will also be decrypted.

- Use cutting and pasting to move files into an encrypted folder. If you use a drag-and-drop operation to move the files, they will not automatically be encrypted in the new folder.

- System files cannot be encrypted.

- Encrypting a folder or file does not protect against deletion. Anyone with delete permission can delete encrypted folders or files.

- Temporary files, which are created by some programs when documents are edited, are also encrypted as long as all the files are on an NTFS volume and in an encrypted folder. It is recommended that you encrypt the Temp folder on your hard disk for this reason. Encrypting the Temp folder ensures that your encrypted documents remain encrypted even during the editing process. If you create a new document or open an attachment in Outlook, the file may be created as an encrypted document in the Temp folder. If you choose to save the encrypted document to another location on an NTFS volume, it will remain encrypted in the new location.

- A recovery policy is automatically implemented when you encrypt your first file or folder so that if you should lose your file encryption certificate and associated private key, a recovery agent can decrypt your file for you.

**EFS Recommendations**

- Encrypt the My Documents folder if this is the place where you save most of your documents. This ensures that your personal documents are encrypted by default.

- Encrypt your Temp folder so that any temporary files created by programs are automatically encrypted.

- Encrypt folders instead of individual files so that if a program creates temporary files during editing, these will be encrypted as well.

- Using the **Export** command from Certificates in Microsoft Management Console (MMC), make backup copies on floppy disk of your file encryption certificate and associated private key. Steps to backup certificates explained further in the reading.  Keep the floppy disk in a secure location. Then, if you should ever lose your file encryption

certificate (through disk failure or any other reason), you can restore
the certificate and associated private key from the floppy disk using the
**Import** command from Certificates in MMC and be able to open your
encrypted files.

**New Features of EFS (Windows XP/2003)**

Compared to Windows 2000, the newer EFS version in Windows XP and
Windows Server 2003 includes several changes. Here's a list of some of the new
features:

- **Encrypted files are marked green so you can easily distinguish them.**

  In Windows Explorer, choose Tools, Folder Options. On the View tab,
  select the option Show Encrypted or Compressed NTFS files in Color.
  This setting makes compressed files appear in blue and encrypted files in
  green.

- **You can share your encrypted files with other individuals.**

  You can share encrypted files with other individuals, but not groups. A
  user with whom you want to share encrypted files must have an
  encryption certificate on your computer. This can be achieved by a couple
  of methods: The user can log onto your computer and encrypt a file; or a
  network user can simply export his or her certificate and you can then
  import the certificate on your computer.

- **EFS offers a client-side caching that's used with the offline folders
  feature.**

  This feature is useful for mobile computers because users can work on
  files even when not connected to the network. The files are cached on the
  user's hard drive. When the user reconnects to the network, the local files
  are synchronized with the files on the network. Unlike Windows 2000, both
  Windows XP and Windows Server 2003 let you encrypt offline files.

- **EFS offers kernel-mode FIPS-compliant cryptography.**

  Federal Information Processing Standard 140-1 (FIPS 140-1) and FIPS
  140-2 are U.S. government standards that provide a benchmark for
  implementing cryptographic software. Some U.S. government agencies
  purchase only products that are FIPS-compliant. In Windows XP/2003,
  you can use a group policy option called system cryptography: Use FIPS
  compliant algorithms for encryption to configure clients to be FIPS-
  compliant.

- **Files can be encrypted even if there's no Data Recovery Agent (DRA).**

**Encrypting File System Tools**

The following tools are associated with Encrypting File System.

**Cipher.exe: Cipher**

Cipher is an operating system command-line tool.

**Version compatibility**   This tool is compatible with Windows 2000, Windows XP, Windows Server 2003.

Allows a user or administrator to display or alter the encryption of files. In addition to encrypting or decrypting a file or folder, Cipher can be used to update the file encryption keys or the keys of the data recovery agent (DRA) should there be a change in the data recovery policy.

**Efsinfo.exe: Encrypting File System Information**

Encrypting File System Information is a Windows Server 2003 Resource Kit command-line tool.

**Version compatibility**   This tool is compatible with Windows 2000, Windows XP, Windows Server 2003.

Encrypting File System Information displays information about files and folders encrypted with Encrypting File System (EFS) on partitions that use the NTFS file system. Options include displaying encryption information about the files and folders in the current folder, recovery agent information, and certificate thumbnail information.

**Xcopy.exe: Xcopy**

Xcopy is a command line tool that ships with Windows Server 2003 and Windows XP Professional.

**Version compatibility**   This tool is compatible with Windows 2000, Windows XP Professional, and Windows Server 2003.

Encrypted files are copied from Web folders in the same way that plaintext files are copied from file shares. The Xcopy command does not require any special

parameters. The file is transmitted in ciphertext and remains encrypted on the local computer if possible. The encryption status for files copied from Web folders is the same as for files copied locally.

**SecPol.msc: Local Security Settings Snap-in**

Local Security Settings is a Microsoft Management Console (MMC) snap-in that ships with Windows Server 2003, Windows 2000 Server, and Windows XP Professional.

**Version compatibility**   This tool is compatible with Windows 2000, Windows XP Professional, and Windows Server 2003.

Local Security Settings is compatible with Windows Server 2003 and Windows 2000 Server, and can be used to EFS data recovery agents on computers running Windows Server 2003, Windows XP Professional, and Windows 2000.

**Encrypting File System Registry Entries**

The following registry entries are associated with Encrypting File System.

- HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\EFS\CurrentKeys

- HKEY_CURRENT_USER\Software\Microsoft\Cryptography\CertificateTemplateCache

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer

The following information is provided as a reference for use in troubleshooting or verifying that the required settings are applied. It is recommended that you do not directly edit the registry unless there is no other alternative. Modifications to the registry are not validated by the registry editor or by Windows before they are applied, and as a result, incorrect values can be stored. This can result in unrecoverable errors in the system. When possible, use Group Policy or other Windows tools, such as Microsoft Management Console (MMC), to accomplish tasks rather than editing the registry directly. If you must edit the registry, use extreme caution.

## How to encrypt and decrypt using the Encrypting File System

The following steps encrypt and decrypt a file or folder using the Encrypting File System.

**Note** These guidelines apply to Windows 2000/ XP/2003.

## Encrypting a folder

Although you can encrypt files individually, we strongly recommend that you designate a specific folder for storing encrypted data.

## Encrypt a folder and its contents

Although you can encrypt files individually, generally it is a good idea to designate a specific folder where you will store your encrypted files, and to encrypt that folder. If you do this, all files that are created in or moved to this folder will automatically obtain the encrypted attribute.

To encrypt a folder and its current contents, follow these steps:

| | |
|---|---|
| 1. | Right-click the folder that you want to encrypt, and then click **Properties**. |
| 2. | In the **Properties** dialog box, click **Advanced**. |
| 3. | The **Advanced Attributes** dialog box displays attribute options for compression and encryption. This dialog box also includes archive and indexing attributes.<br><br>**Note** Although the NTFS file system supports both compression and encryption, it does not support both at the same time. This means that you can only select one or the other. A file or folder cannot be both encrypted and compressed at the same time.<br><br>To encrypt the folder, click to select the **Encrypt contents to secure data** check box, and then click **OK**. |
| 4. | Click **OK** to close the **Advanced Attributes** dialog box. |
| 5. | If the folder you chose to encrypt in steps 1 to 3 already contains files, a **Confirm Attribute Changes** dialog box will appear.<br><br>You can choose to encrypt only the folder so that all files subsequently moved to the folder or created in this folder will be encrypted. If you want to also encrypt all the contents of this folder, click **Apply changes to this** |

**folder, subfolders, and files**, and then click **OK**.

## Decrypting a folder

To decrypt a folder, use basically the same process but in reverse order:

1. Right-click the folder that you want to decrypt, and then click **Properties**.

2. Click **Advanced**.

3. Click to clear the **Encrypt contents to secure data** check box to decrypt the data.

4. Click **OK** to close the **Advanced Attributes** dialog box.

5. Click **OK** to close the **Properties** dialog box.

6. If the folder has files in it, the **Confirm Attribute Changes** dialog box appears. You can choose to decrypt only the folder. However, this will not decrypt any files currently contained in the folder.

   If you want to decrypt all the contents of this folder, click **Apply changes to this folder, subfolders, and files**, and then click **OK**.

## How to enable Encrypting File System file sharing

In Microsoft Windows XP and 2003, EFS supports file sharing of encrypted files among multiple users. With this support, you can give individual users permission to access an encrypted file. The ability to add additional users is restricted to individual files. Support for multiple users on folders is not provided in either Microsoft Windows 2000 or Windows XP. Also, support for the use of groups on encrypted files is not provided by EFS.

After a file has been encrypted, file sharing is enabled through a new button in the user interface. A file must be encrypted first and then saved before additional users can be added. Users can be added either from the local computer or from the Active Directory directory service if the user has a valid certificate for EFS. The ability to add additional users is restricted to individual files. Support for multiple users on EFS encrypted folders is not provided. Also, only individual users can be added to files. Support for the use of groups on encrypted files is not provided by EFS.

**How to encrypt a file for multiple users**

**Note** This procedure applies to Windows XP only. You cannot encrypt a file for multiple users in Windows 2000.

To do this, follow these steps: (Window XP/2003)

| | |
|---|---|
| 1. | Start Microsoft Windows Explorer, and then select the encrypted file that you want to add additional users to. |
| 2. | Right-click the encrypted file, and then click **Properties**. |
| 3. | Click **Advanced** to access the EFS settings. |
| 4. | Click **Details** to add additional users. |
| 5. | Click **Add**. The **Add** dialog box will display any other EFS-capable certificates in your personal store or those of any other users who may be in your "Other People" and "Trusted People" certificate stores.<br><br>If you do not see the user who you want to add, click **Find User** to search Active Directory. The **Select User** window appears. A dialog box displays valid EFS certificates in Active Directory based on your search criteria. If no valid certificate is found for that user, a message will inform you that there are no appropriate certificates for the selected user. In this case, the intended users must send you a copy of their certificate for you to import. You can then add them to your encrypted file. |
| 6. | Select the certificate of the user who you want to add, and then click **OK**. You will be returned to the **Details** tab, and the tab will show the multiple users who will have access to the encrypted file and the users' EFS certificates. |
| 7. | Repeat this process until you have added all the users who you want to add. Click **OK** to register the change and continue. |

**Note** Any user who can decrypt a file can also remove other users if the user who does the decrypting also has write permissions on the file

**Additional information**

**How files are encrypted**

Files are encrypted through the use of algorithms that essentially rearrange, scramble, and encode the data. A key pair is randomly generated when you encrypt your first file. This key pair is made up of a private and a public key. The key pair is used to encode and decode the encrypted files.

**Why does EFS use a public key/private key algorithm to encrypt File Encryption Keys (FEKs), and Data Encryption Standard (DESX) to encrypt file data?**

Because DESX uses the same key to encrypt and decrypt data, it is a symmetric encryption algorithm. Symmetric encryption algorithms are typically very fast, which makes them suitable for encrypting large amounts of data, such as file data. However, symmetric encryption algorithms have a weakness: You can bypass their security if you obtain the key. If multiple users want to share one encrypted file protected only by DESX, each user would require access to the file's FEK. Leaving the FEK unencrypted would obviously be a security problem, but encrypting the FEK once would require all the users to share the same FEK decryption key—another potential security problem.

If the key pair is lost or damaged and you have not designated a recovery agent, and then there is no way to recover the data.

**Why you must back up your certificates?**

Because there is no way to recover data that has been encrypted with a corrupted or missing certificate, it is critical that you back up the certificates and store them in a secure location. You can also specify a recovery agent. This agent can restore the data. The recovery agent's certificate serves a different purpose than the user's certificate.

**How to back up your certificate**

To back up your certificates, follow these steps:

| | |
|---|---|
| 1. | Start Microsoft Internet Explorer. |
| 2. | On the **Tools** menu, click **Internet Options**. |
| 3. | On the **Content** tab, in the **Certificates** section, click **Certificates**. |

| 4. | Click the **Personal** tab. **Note** There may be several certificates present, depending on whether you have installed certificates for other purpose. |
|---|---|
| 5. | Select one certificate at a time until the **Certificate Intended Purposes** field shows **Encrypting File System**. This is the certificate that was generated when you encrypted your first folder. |
| 6. | Click **Export** to start the **Certificate Export Wizard**, and then click **Next**. |
| 7. | Click **Yes, export the private key** to export the private key, and then click **Next**. |
| 8. | Click **Enable Strong protection**, and then click **Next**. |
| 9. | Type your password. (You must have a password to protect the private key.) |
| 10. | Specify the path where you want to save the key. You can save the key to a floppy disk, another location on the hard disk, or a CD. If the hard disk fails or is reformatted, the key and the backup will be lost. (If you back up the key to a floppy disk or CD, you must store that disk or CD in a secure location.) |
| 11. | Specify the destination, and then click **Next**. |

The encryption algorithms available to EFS depend on which version of Windows is running on the computer:

- Windows XP with SP1 or later can encrypt or decrypt files using DESX, 3DES, or AES.

- Versions of Windows XP Professional earlier than SP1 can use the DESX or the Triple-DES (3DES) algorithm for EFS encryption and decryption.

- Windows 2000 Professional and Windows 2000 Server use the DESX algorithm for EFS encryption and decryption

**Cryptographic Service Providers (Windows XP/2003)**

The public-private key pairs for EFS users and recovery agent accounts are obtained from the Microsoft Base cryptographic service provider (CSP). These CSPs are included with Windows Server 2003 and Windows XP Professional.

- Depending on the CSP you select, you can select one of three encryption algorithms to encrypt and decrypt the contents of files:

- **Triple-DES (3DES).** 3DES, which is compliant with Federal Information Processing Standards (FIPS 140-1 Level 1), offers significantly stronger encryption using a 128-bit or 168-bit key. 3DES is enabled through a Group Policy setting. All EFS FIPS mode encryption processes are completed using 3DES.

- **DESX.** An enhanced variant of the Data Encryption Standard (DES).

- **Advanced Encryption Standard (AES) algorithm.** This is the default encryption standard for Windows Server 2003 and Windows XP Professional with Service Pack 1 installed. AES uses a 256-bit key for encryption and decryption.

If you've backed up your private key and EFS certificate, you can always restore it to recover your encrypted files. This is true both in Windows 2000 and Windows XP/2003. The same is true if you have a DRA configured at the time the files were encrypted, because the DRA can recover your files for you. However, things get rather messy when a user forgets the password.

In Windows 2000, if a user forgets a password, the administrator can reset the password and it has no effect on the user's encrypted files. This is true whether the user logs onto the domain or to a standalone computer in a workgroup. However, a hacker can easily use a third-party tool such as Ntpassword to replace the password hash in the local Security Accounts Manager (SAM)—and gain complete access to the user's encrypted files by logging on as that user.

In Windows XP, Microsoft has improved the security on EFS certificates; the certificate's private keys are now protected with your local account's password. If a user forgets the password and the administrator resets the password for a domain account, no harm is done; the user can continue to access the encrypted files.

**Section 7 – Account Security**

The account is the central unit of security on Microsoft Windows 2000, Windows XP, and Windows 2003 computers and the applications that run on them. Rights and permissions are assigned to accounts and checked by a resource such as a file or a folder at the time of access. It is important to understand that a user and a user account are different entities. Anyone who possesses the credentials associated with a user account can use that account, despite the name on it. A computer can secure and audit access to resources based on user accounts only, not on the identity of the person using the account.

IAW AR 25-2 paragraph 3-3, administrators will

- Manage and review user accounts, access, and logins and suspend or terminate accounts in accordance with local policy.
- Remove inactive accounts that exceed 45 days and departing users' accounts before departure.
- Manage, enforce, and audit all accounts passwords, permissions, inactivity, and suspension policies.
- Remove or disable all default, guest, and service accounts in information systems or network devices, and rename administrative accounts as applicable.
- Use separate accounts for SA/NA privileged level and general user access.

**Password Policy**

Passwords are an important step in a security plan for your network. Users may see passwords as a nuisance; however, the security of your enterprise relies on a combination of password length, password uniqueness, and password lifespan. These three items help defend against dictionary attacks and brute force attacks. A dictionary attack occurs when a malicious user tries known words that are in the dictionary and a number of common password names to try and guess a password. A brute force attack occurs when a malicious user tries all of the possible permutations until one is successful.

Passwords must be vigilantly safeguarded.  Administrators will enforce password policy through implementation or enhancement of native security mechanisms. Administrators will also implement other authentication techniques (for example biometrics, access control devices, or smart cards) as viable alternatives in conjunction with, or in place of password as tested or approved by NETCOM and CIO/G-6.  All default, system, factory installed, function-key embedded, or maintenance passwords will be removed or changed.  Authenticate user access to all systems with a minimum of a userid and an authenticator.  An authenticator may be something the user knows (password), something the user have (CAC card), or something that you are (biometric).  System administrators and network

administrators will implement procedures for user authentication or verification before resetting passwords or unlocking accounts.

In accordance with AR 25-2 paragraph 4-12, the following are true concerning passwords:

- Passwords will not to be shared.  Only the holder is the only authorized user of that password.
- Passwords will change no less frequently than every 90 days and password expiration will be not more than 150 days.
- Passwords will have a minimum requirement of 10-character case-sensitive.  Passwords or phrases longer than 10 characters are recommended when supported by the information system.
- Passwords will be mixed of uppercase letters, lowercase letters, numbers, and special characters, including at least two of each of the four types of characters (for example, x$TIoTBn2!) and can be user generated.
- Passwords will not include such references as social security numbers (SSNs), birthdays, USERIDS, names, slang, military acronyms, call signs, dictionary words, consecutive or repetitive characters, system identification, or names; neither will they be easy to guess (for example, mypassword, abcde12345).
- Password history configuration will prevent reutilization of the last 10 passwords when technically possible.
- The use of password generating software or devices is authorized as a memory aid when it randomly generates and enforces password length, configuration, and expiration requirements; protects from unauthorized disclosure through authentication or access controls; and presents a minimal or acceptable risk level in its use.

Within 72 hours of any failed log-on and user lockout, IA personnel will verify the reason for failure and implement corrective actions or report the attempted unauthorized access.  The SA will maintain a written record of all reasons for failure for 1 year.  Reinstate accesses only after the appropriate IA (for example, SA/NA) personnel have verified the reason for failed log-on attempts and have confirmed the access-holder's identity.  Permit automatic account unlocking (for example, established time period elapsed) as an exception only, based on sensitivity of the data or access requirements.

**Screensaver Policy**

Administrators will enforce the use of password-protected screen savers, screen locks, or other lockouts feature to prevent unauthorized access on all information systems during periods of temporary non-use; configure such mechanisms to automatically activate when a terminal is left unattended for no longer than 10 minutes.  Establish a shorter period if appropriate, such as in a multinational work area.  It is recommended three to five minutes.

Use password protected screen savers, screen locks, or other lockout features to prevent unauthorized access on all ISs during periods of temporary non-use.

## Administrator Account

Rename the default administrator account "Administrator" to something harder to guess and remove the information in the description block.  This will prevent people from guessing your administrator account.  Make sure you remember the new administrator account and password.

Next, create a decoy account.  Create a new user called "Administrator", and make sure it does NOT belong to any groups.  In another words, when you click on the "Member of" tab in the user properties in the User Management window, you should not see any groups listed.  If you do, remove them.  This will make sure this decoy account named "Administrator" has no access to the server.

If you have the Audit for logon/logoff turned on, you will be able to detect any logon/logoff activities by the decoy "Administrator" user account.  You can detect these activities by using Event Viewer to check Security Logs.  This will give you some indication of hacking activities.

## Security Subsystem Components

Each user, computer, or group account is a security principal in Windows 2000, Windows XP and Windows 2003. Security principals receive permissions to access resources such as files and folders. User rights, such as interactive logons, are granted or denied to accounts directly or via membership in a group. The accumulation of these permissions and rights define what security principals can and cannot do when working on the network.

Local Security Authority (LSA) – is a protected subsystem that authenticates and logs users on to the local computer. In addition, LSA maintains information about all aspects of local security on a computer (these aspects are collectively known as the local security policy), and it provides various services for translation between names and security identifiers (SIDs).

The security subsystem keeps track of the security policies and the accounts that are in effect on a computer system. In the case of a domain controller, these policies and accounts are the ones that are in effect for the domain in which the domain controller is located. These policies and accounts are stored in Active Directory.

The local security policy identifies the following:

- Which domains are trusted to authenticate logon attempts?
- Who can have access to the system and in what way (for example, interactively, over the network, or as a service)?
- Who is assigned what rights?
- What security auditing is performed?
- What the default memory quotas are for paged and non-paged memory pool usage.

## LSA Architecture
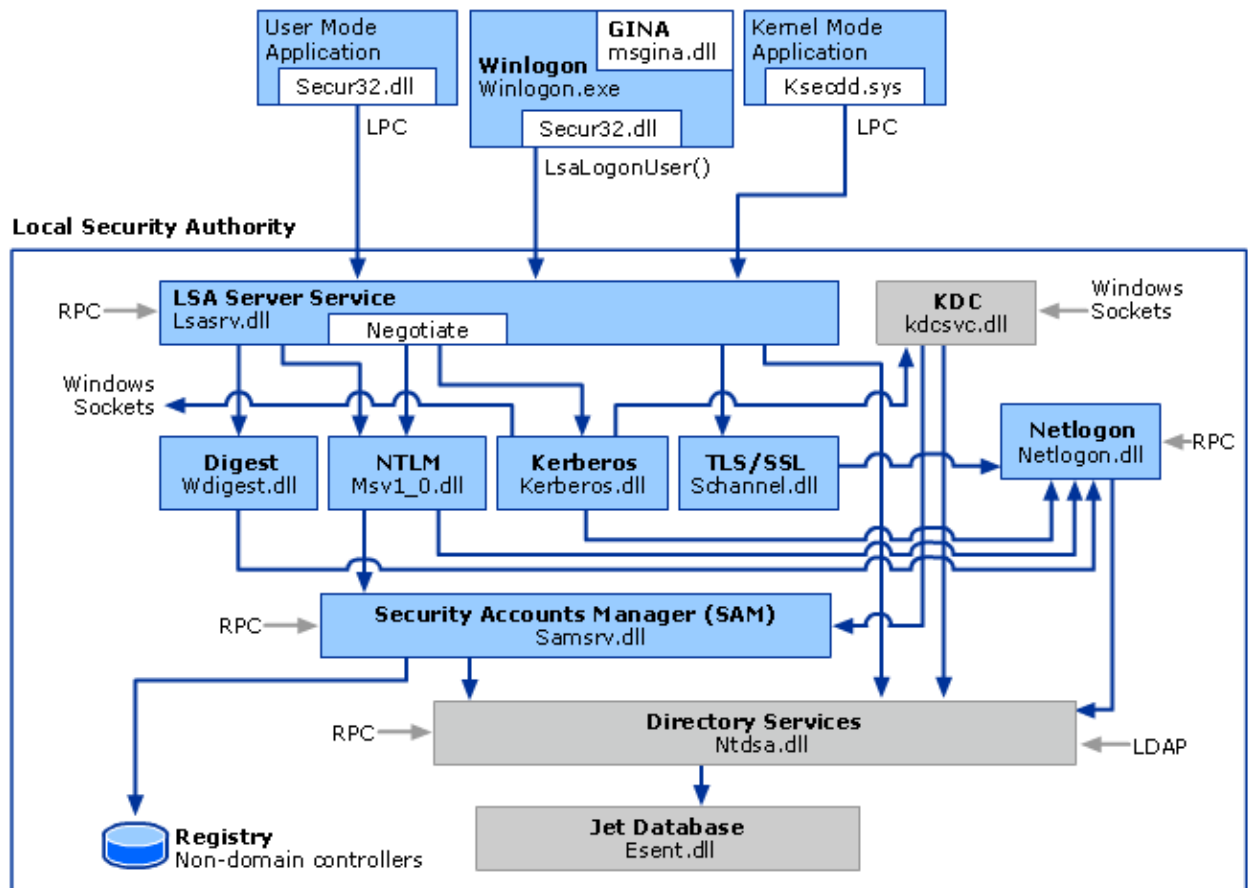


The LSA security subsystem provides services for validating access to objects, checking user rights, and generating audit messages. A local procedure call (LPC) occurs between components on the same system. A remote procedure call (RPC) occurs between components on different systems, as do LDAP communications.

In general, the LSA performs the following functions:

- Manages local security policy.

- Provides interactive user authentication services.
- Generates access tokens.
- Manages the audit policy and settings.

**Security Accounts Manager** – is responsible for maintaining all user and group accounts.  It accesses the SAM Database or the Active Directory database, which contains usernames, passwords, group and privilege information.  SAM is part of the *Isass.exe* process.  The local *SAM* manages accounts used only on that computer, while the domain *SAM* manages accounts, both computer and user, for the domain. The Active Directory is only available in Windows 2000 and Windows 2003 domain controllers. The SAM Database exists on machines that are not domain controllers.  It contains all user account information for that machine.  The SAM Database is found in the folder %systemroot%/system32/config, and the database file itself is called SAM.  It is loaded into the registry upon boot.  It is encrypted and the contents cannot be displayed without the use of third party tools.

**Security Identifier (SID)** – is a value of variable length that is used to uniquely identify a security principal or security group.

Each account or group has a unique SID that is issued by an authority, such as a Windows domain controller, and stored in a security database. The system generates the SID that identifies a particular account or group at the time the account or group is created. When a SID has been used as the unique identifier for a user or group, it can never be used again to identify another user or group.

In addition to the uniquely created, domain-specific SIDs that are assigned to specific users and groups, there are well-known SIDs that identify generic groups and generic users. For example, the *Everyone* and *World* SIDs identify a group that includes all users. Well-known SIDs have values that remain constant across all operating systems.

SIDs are a fundamental building block of the Windows security model. They work together with specific components of the authorization and access control technologies in the Windows 2000, Windows XP, and Windows 2003 security infrastructure to help protect access to network resources and provide a more secure computing environment.

While users reference their accounts by the user name or universal principal name (UPN), the operating system internally references accounts by their security identifiers (SIDs). For domain accounts, the SID of a security principal is created by concatenating the SID of the domain with a relative identifier (RID) for the account. SIDs are unique within their scope (domain or local) and are never reused. This is an example of a SID:

**S-1-5-21-833815213-1531848612-156796815-1105**

SIDs have several components:

**Revision**

This value indicates the version of the SID structure used in a particular SID. The revision value is 1 in Windows 2000, Windows XP, and Windows 2003.

**Identifier authority**

This value identifies the highest level of authority that can issue SIDs for this particular type of security principal. The identifier authority value in the SID for an account or group in Windows 2000, Windows XP, and Windows 2003 is 5 for the NT Authority.

**Subauthorities**

The most important information in a SID is contained in a series of one or more subauthority values. All values up to but not including the last value in the series collectively identify a domain in an enterprise. This part of the series is known as the domain identifier. The last value in the series identifies a particular account or group relative to a domain. This value is the RID. In the example just given, this value is 1105.

By default, several security principals are created during installation of the operating system or domain; the SIDs for these accounts are called well-known SIDs. Table 3-1 lists the well-known SIDs for Windows 2000, Windows XP, and Windows 2003.

Well-known SIDs:

- SID: S-1-5-*domain*-500
  Name: Administrator
  Description: A user account for the system administrator. By default, it is the only user account that is given full control over the system.
- SID: S-1-5-*domain*-501
  Name: Guest
  Description: A user account for people who do not have individual accounts. This user account does not require a password. By default, the Guest account is disabled.
- SID: S-1-5-*domain*-502
  Name: KRBTGT
  Description: A service account that is used by the Key Distribution Center (KDC) service.

**Access Token** - is a protected object that contains information about the identity and privileges associated with a user account.

Every time a user logs on, the system creates an access token for that user. The access token contains

- The user's SID
- The SIDs for any groups the user belongs to
- The user's privileges.

This token provides the security context for whatever actions the user executes on that computer. When a user logs on interactively or tries to make a network connection to a computer running Windows, the logon process authenticates the user's logon credentials. If authentication is successful, the logon process returns a SID for the user and a list of SIDs for the user's security groups. The LSA on the computer uses this information to create an access token — in this case, the primary access token — that includes the SIDs returned by the logon process as well as a list of privileges assigned by local security policy to the user and to the user's security groups.

After LSA creates the primary access token, a copy of the access token is attached to every process and thread that executes on the user's behalf. Whenever a thread or process interacts with a securable object or tries to perform a system task that requires privileges, the operating system checks the access token associated with the thread to determine the level of authorization for the thread.

There are two kinds of access tokens, primary and impersonation. Every process has a primary token that describes the security context of the user account associated with the process. A primary access token is typically assigned to a process to represent the default security information for that process. Impersonation tokens, on the other hand, are usually used for client/server scenarios. Impersonation tokens enable a thread to execute in a security context that differs from the security context of the process that owns the thread.

**Security Descriptors** –   Security descriptors include information about who owns an object, who can access it and in what way, and what types of access are audited. Security descriptors, in turn, contain the access control list (ACL) of an object, which includes all of the security permissions that apply to that object. An object's security descriptor can contain two types of ACLs:

A discretionary access control list (DACL) that identifies the users and groups who are allowed or denied access

A system access control list (SACL) that controls how access is audited.  You can use this access control model to individually secure objects such as files and folders, Active Directory objects, registry keys, and printers, as well as devices, ports, services, processes, and threads. Because of this individual control, you can adjust the security of objects to meet the needs of your organization,

delegate authority over objects or attributes, and create custom objects or attributes that require unique security protections to be defined.

Access tokens are created by the security system, and they contain security information about users who have logged on and been authenticated. When a user requests access to an object, the access token of the account requesting access is compared to the object's DACL.  Each permission that an object's owner grants to a particular user or group is stored as an access control entry (ACE) in a DACL that is part of the object's security descriptor. In the user interface, ACEs are displayed as Permission Entries. If auditing is configured for an object, the object's security descriptor also contains a SACL that controls how the security subsystem audits attempts to access the object.

The following figure shows the relationship of security descriptors and ACLs to other key components of the authorization and access control model.

**Relationship of Security Descriptors and ACLs to Other Authorization and Access Control Components**
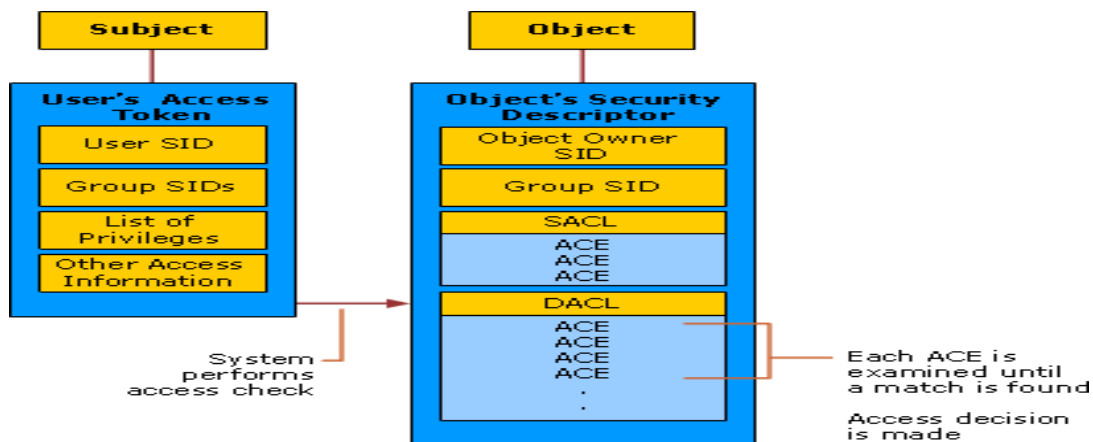


**Group Policy**

Window's 2000, XP, and 2003 Group Policy isn't simply a written guideline, such as a warning to prevent users from installing unauthorized software. Group Policy is a set of rules that Windows 2000, XP and 2003 implements, using Registry changes, when a computer starts or when a user logs on. The policies become part of the user environment, imposing restrictions on what the user can and can't do.

What can you do with Group Policy? With a Group Policy, you can

- Run startup script for a computer and user logon scripts

- Configure a user's desktop by removing or restricting the options to run applications, connect on the network, or even choose wallpaper.
- Set security restrictions, security options, and control access to network resources.
- Manage users' desktops by regulating which applications users can run
- Push scripts out to computers which are then automatically executed.
- Reconfigure NTFS permissions and audit settings
- Set password and account lockout policies
- Distribute IPSec encryption settings to all workstations and servers
- Change EFS recovery agents
- Control which Certification Authorities users should trust
- Set any number of registry values.

Even without an Active Directory infrastructure, many of the security settings stored in Group Policy Objects can be saved in a security template and manually applied with the Security Configuration and Analysis Tool.

You can set security policy at different levels in the AD structure. Policies that you set at a high level in the directory tree, for example, can flow down to lower levels such as organizational units (OUs). Optionally, you can modify or override policies at a lower level. Group Policy now controls software distribution, limiting applications to certain clients or computers.

Windows 2000, XP and 2003 don't use NT's ntconfig.pol file, which NT needed to replicate to the backup domain controllers. Instead, you create a Group Policy Object (GPO). A GPO is a virtual storage location for your policies. You can place different policies in different GPOs, and you can apply each GPO to selected users or computers. (You apply GPOs to only users or computers, but you can also filter the effects of GPOs by groups.) Replication of the policies occurs under the control of the Windows File Replication Service (FRS). You can associate one GPO with many AD containers, and each AD container can have multiple GPOs associated with it.

Windows 2000, XP and 2003 store Group Policy information in two locations: the Group Policy Container (GPC) and the Group Policy Template (GPT). The GPC is the AD object associated with the GPO. The GPC and GPT contain the GPO's version and status information. The GPT is a set of files residing in the \sysvol folder, which you'll find on your domain controllers. (Don't confuse the GPT with the System Volume Information folder. The policies in \sysvol reside under \*systemroot*\sysvol\sysvol\*domainname*\policies.) In the GPT, you'll find information about administrative templates, security, scripts, and software installation.

Before you start creating GPOs, consider where you need to apply the policy. You can apply a group policy to a

- Site
- Domain
- Organizational unit (OU)
- Child organizational unit (OU)

Does the policy apply to all of your users or computers? If so, perhaps you need to apply the policy at the site level. If the policy is relevant to only one domain or to users within one OU, applying the policy at the domain or OU level might be more appropriate.

When a user logs on, Windows 2000, XP and 2003 evaluate policies starting at the top of the AD structure and working down. The order of evaluation is

- Local group policies
- Site
- Domain
- OU

At each level, you can set a policy as

- Enabled – means the changes will occur at the time of evaluation.
- Disabled – means the changes will not occur at the time of evaluation.
- Not Configured – means that at a particular level, no setting changes will occur at the time of evaluation.

By default, each container inherits GPO settings from the container above it. However, a setting in a lower container, such as an OU, can override a setting at a higher level. Therefore, if you set a policy in the parent OU, but you don't configure it in the child OU, the child OU will inherit the parent setting. If you configure a similar policy at both parent and child, both settings will apply without conflict. But when the parent and child OU policies conflict, the child policy takes precedence, and the OU won't inherit the parent policy setting. You can apply a broad set of policies to your users, and then modify policies for specific subgroups in your organization as necessary.

Sometimes, you will not want child containers to change your GPO at a lower organizational level. You might have corporate policies that you don't want to change at any level. For example, to ensure that users install only software with valid certificates, you might want to enforce the Disable changing certificate setting. The **No Override** option, which applies to the entire GPO, prevents any child container from overriding the policy. Therefore, you need to place all your corporate, nonnegotiable policies into one GPO, and then set the No Override option. You can place other policies that need to vary by OU in another GPO with the No Override turned off.

Occasionally, you might have an OU that needs a separate set of policies—corporate policies won't work. For example, the majority of users in your company might be fairly relaxed about policies—except for the accountants, who want more rigid policies. The Accountants OU can set the **Block Inheritance** option. That way, the accountants can set their own policies and avoid inheriting any policies from the parent domain or OU. The No Override option takes precedence over Block Inheritance, so an administrator lower in the hierarchy can't block your corporate policies.

When you're planning policies, the best practice is to start at the top level of your AD structure with the broadest policies, then work your way down to the lower levels for more specific policies that apply to selected user groups or computers in specific OUs. However, you need to consider factors other than the combination of policies at each hierarchy level. The AD structure's depth can affect your planning. Because policy settings at one level modify the inherited settings from the level above, processing all the policies at every level from the top down to a user takes some time. Users at the bottom of the hierarchy might find that logging on takes longer than they expect.

Another consideration is the network traffic that might generate when users connect. A GPO associated with a site affects every computer in the site, regardless of which domain the computers belong to. Therein lies the obvious benefit of a site policy. However, the GPO resides in only one domain, and you might have multiple domains in your site. Therefore, to obtain the policy, all the computers in every domain need to contact a domain controller in the domain that contains the GPO. This necessity creates additional network traffic and a heavy load on the domain controllers. Creating identical GPOs at the domain level—so that each computer can obtain policies from its own domain controller—is often the way to go. To improve performance, you can disable computer or user settings per GPO. You can also set up the GPO so that the system processes it only if its version number has changed since the most recent startup or logon.

Unlike NT 4.0 system policies, some Group Policy settings affect both users and computers. In NT, a policy was either a computer policy that integrated into the HKEY_LOCAL_MACHINE Registry key or a user policy that merged with the HKEY_CURRENT_USER Registry key. Windows 2000, XP and 2003 lets you specify some policies either for the computer or for the user. This freedom increases the possibility that policies will apply to both the user and the computer—along with the possibility that one policy will overwrite another. Knowing the order in which Windows 2000, XP and 2003 processes policies is helpful.

When a computer starts, Windows 2000, XP and 2003 process any Group Policy settings for that computer, and startup scripts run. To ensure that the computer policies are in effect when the user logs on, the Group Policy settings for that

computer activate before the logon screen displays. Finally, any individual logon scripts run after the system processes the Group Policy logon scripts.

Another difference between Windows 2000, XP and 2003 and NT 4.0 is that the user no longer needs to log off and log on again to receive new policy settings. (Therefore, a user can't retain old policy settings by never logging off.) By default, client computers check for new policies every 90 minutes—with a randomized offset of plus or minus 30 minutes, so that the computers don't all check simultaneously. Domain controllers renew their policy data every 5 minutes. The only exceptions are software-installation and folder-redirections settings, which Windows 2000, XP and 2003 processes only when the computer starts or a user logs on. If you need to notify users about the availability of new software in a more timely manner, consider Microsoft Systems Management Server (SMS).

You can use the Microsoft Management Console's (MMC's) Security Templates snap-in to build different templates that you can import into Group Policies. You can either create a new policy from scratch or modify one of the built-in policies. After you decide which template to use, you can import the template settings into your GPO using Group Policy Editor (GPE) by right-clicking Computer Configuration, Windows Settings, Security Settings and choosing Import Policy. This process applies all the settings you configured in the template to all the computers in the container (e.g., site, domain, OU) that you link the Group Policy to.

You can use the MMC's Security Configuration and Analysis snap-in to verify that the security settings you apply with Group Policy are in use. Before you perform an analysis, create a database to store the results. After you create and open the database and choose the template containing the settings that you want to apply to a specific machine, right-click the snap-in and choose Analyze Computer Now to check the actual security settings against the desired settings. You can also use Security Configuration and Analysis to apply the security template to the machine, but it's better to use Group Policy. If you use Security Configuration and Analysis to apply the settings, a user can come behind you and change the settings. With Group Policy, if a user changes a security setting, it changes back to its original value the next time Win2K applies the policy.

**Anonymous Users / Everyone Group**

Anonymous users (users or services that access resources over a network connection by using a null user account name, domain and password) are automatically added to the Anonymous Logon built-in security group. In earlier versions of Windows, members of the Anonymous Logon security group are able to access many resources. In some cases, if administrators are not aware that members of the Anonymous Logon security group are included as members of the Everyone security group, anonymous users may be granted access to resources that are only intended for authenticated users.

In Windows XP and later, the Anonymous Logon security group has been removed from the Everyone security group. This modification helps to limit the number of network resources that are available by default to anonymous users, and to simplify network administrators' control of anonymous user access. Because the Everyone group no longer includes anonymous users, it is easier for administrators to configure a secure system for the following reasons:

- The default ACLs on earlier versions of Windows (particularly Windows NT 4.0) that enable the Everyone security group to access resources, and potentially expose the site to attack, do not grant access to anonymous users after the computer is upgraded to Windows XP.
- Anonymous users are not granted access to resources that the administrator is unaware of.
- Anonymous users can be explicitly granted access to specific resources through the clearly named Anonymous Logon security group.

Note: this security enhancement is present only on computers that are running Windows XP or later. Therefore, only anonymous users that are attempting to access resources that are hosted on computers that are running Windows XP or later are affected.
On Windows Server 2003 domain controllers, to grant Anonymous access, you must include the Everyone and Anonymous groups in the Pre-Windows 2000 Compatible Access group.

NOTE: If you upgrade a <u>Windows 2000</u> domain controller to Windows Server 2003 and you had already added the Everyone group to the Pre-Windows 2000 Compatible Access group, the Anonymous group is automatically added during the upgrade.
NOTE: If you promote a Windows Server 2003 computer to a domain controller using DCPROMO, check Permissions compatible with pre-Windows 2000 servers to add both the Everyone and Anonymous groups to the Pre-Windows 2000 Compatible Access group.

If you upgrade Windows 2000 to Windows XP, the resources granted to the Everyone group are no longer available to Anonymous users.

If you need Anonymous access in Windows XP, explicitly add the Anonymous group to the ACL of the objects that require it. If you have difficulty in determining which objects require Anonymous access, you could include the Anonymous group in the Everyone group.  This requires the support of the **everyoneincludesanonymous** Value Name, a REG_DWORD data type, at **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa**. When the access token for an Anonymous user is created and the data value of the **everyoneincludesanonymous** Value Name is 0, the default, the Local Security Authority (LSA) of Windows XP does NOT include the SID of the Everyone group in the Anonymous user's access token. If the **everyoneincludesanonymous**

data value is 1 when the access token for an Anonymous user is created, the LSA includes the SID of the Everyone group.

You can also use Group Policy to set the **everyoneincludesanonymous** Value Name:

- Open the Local Security Policy from Administrative Tools, or on a domain controller, the Domain Security Policy.
- Expand Security Settings / Local Policies / Security Options.
- Double-click <u>Network</u> access: let Everyone permissions apply to anonymous user.
- Press Enabled to allow Anonymous users to be members of the Everyone group, which sets **everyoneincludesanonymous** to 1. Press Disabled to revert to default Windows XP behavior, setting **everyoneincludesanonymous** to 0.

## Section 7 - AUDITING

## What is Auditing?

Auditing is a process by which Windows lets you know what's going on with both the system itself and with the users.   Auditing is a general tool that has been around since the days of Windows NT. Auditing is very similar to Performance Monitor, in that it waits for a specific event to occur, and then reports on it within the Event Viewer. Instead of waiting for system performance events, auditing usually tracks the success or failure of system and security events. Traditionally, auditing was most frequently performed for user logon/logoff (to track tardy employees) and sensitive file access (to see who and how often file access occurred). More recent enhancements to auditing allow the system to automatically report changes to user accounts and permissions, as well as changes to group policies, trusts, domains, and every AD-based object in the system. This is a tremendous step forward, because it essentially allows for auditing for nearly every system and domain-critical object that's out there.

Auditing falls into 3 main areas:

- Vulnerability Management:  checking the configuration of a system or systems against a defined baseline, and perhaps ensuring that the applied baseline meets current best security practice recommendations.
- Threat Management:  the real-time detection of a threat or actual intrusion.
- Collecting and analyzing events:  to reveal security information related to the actual use or abuse of a given system or group of systems.

Auditing with Windows 2000, XP and 2003 are configured in several different ways, all depending upon what needs to be audited, and where that objects resides. Generally, the first step is to enable the specific type of auditing through the audit policy, which will usually begin the audit process at that point. Auditing is generally turned on through a security policy, which is another part of Group Policy. These security policies are generally accessed through Administrative Tools.

- **Audit Account Logon Events:** Tracks user logon and logoff events.
- **Audit Account Management:** Reports changes to user accounts.
- **Audit Directory Service Access:** Reports access and changes to the directory service. If the system is a member server or XP system, directory service is NTLM-based, and consists of user accounts and group policies.
- **Audit Logon Events:** Reports success/failure of any local or remote access-based logon.
- **Audit Object Access:** Reports file and folder access. Must be implemented here, and then the individual file/folder must be configured for auditing within its properties in order to fully enable this feature.

- **Audit Policy Change:** Reports changes to group policies.
- **Audit Privilege Use:** Related to Audit Object Access: reports when permissions are utilized such as read, or full control.
- **Audit Process Tracking:** Reports process and program failures. Not security related.
- **Audit System Events:** Reports standard system events. Not security related.

## Why should you audit?

As you're no doubt aware, Windows 2000, XP and 2003 have a very robust security system. However, all the security in the world does little good if you don't know how to check up on it. That is where auditing comes in. No security strategy is complete without a comprehensive auditing strategy. More often than not, organizations learn this the hard way—only after they have experienced a security incident. Without an audit trail of actions made by the intruder, it is almost impossible to successfully investigate a security incident. As part of your overall security strategy, you must determine which events you need to audit, the level of auditing appropriate for your environment, how the audited events will be collected, and how they will be reviewed. There are several reasons to enable auditing and monitor audit logs:

- To create a baseline for normal network and computer operations
- To detect attempts to break into the network or computer
- To determine which systems and data have been compromised during or after a security incident

In addition, by regularly monitoring audit logs, especially by using automatic event monitoring software, you can help prevent further damage to networks or computers once an attacker has penetrated the network but has not yet inflicted widespread damage. To put auditing in a real-world perspective, consider this: Setting up Windows security without using auditing is like installing an expensive home security system without any type of alarm. Sure, the locks will keep some intruders out; but if someone breaks into your house, wouldn't you like to know about it? The same principle applies to Windows. Setting permissions will keep most of your users from doing things they aren't supposed to, but if a user or an outside intruder does happen to get past your security settings, it would be nice to be aware of the fact.

## What governs auditing?

AR 25-2 Information Assurance
AR 380-53 Information Systems Security Monitoring
DoD 8500.2 Information Assurance (IA) Implementation

**What should you audit?**

In Windows 2000, XP and 2003, you can audit just about any action by either the system or by a user. Which OS events should you audit? The easy answer to this question is all of them. Unfortunately, auditing all OS events would require enormous system resources and could negatively affect system performance. Bear in mind that the more you audit, the more events you generate and the more difficult it can be to spot critical events. If you plan to monitor the audited events manually or if you do not have a clear understanding of how to read audit logs, it can be extremely difficult to isolate potential malicious events from innocuous ones. You will need to work with other security specialists—ideally those who specialize in forensics or computer crime investigations—and IT decision makers to determine the OS events to audit.

In Microsoft Windows 2000, XP and 2003, audit events can be split into two categories: success events and failure events. A success event indicates that the action or operation has been successfully completed by the OS, whereas a failure event shows that the action or operation was attempted but did not succeed. Failure events are useful in tracking attempted attacks on your environment; success events are much more difficult to interpret.  By default, none of Windows 2000 and XP auditing features is turned on. However, Windows 2003 Server has by default audit account logon and audit logon events turned on.  Also by default, Windows 2003 Server has audit object access, audit privilege use, and audit process tracking turned off.  The following services are turned on depending on the status of the server (i.e. domain controller or member server): Audit Account Management, Audit Directory Service Access, Audit Policy Changes, and Audit System Event. For DoD systems, you will audit the success or failure of events such as logins, object access, privilege use, account management, policy changes, system events and process tracking.  For a more stringent guidance, administrators should check their local security policy.

Enabling system auditing can inform you of actions that pose security risks and possibly detect security breaches.  The following are some vulnerabilities and countermeasures that auditing will assist you with:

| Vulnerability | Countermeasure |
|---|---|
| Hacker-type break-in using random passwords | Enable failure auditing for log on and log off events. |
| Break-in using stolen password | Enable success auditing for log on and log off events. The log entries will not distinguish between the real users and the phony ones. What you are looking for here is unusual activity on user accounts, such as logons at odd hours |

| | |
|---|---|
| | or on days when you would not expect any activity. |
| Misuse of administrative privileges by authorized users | Enable success auditing for use of user rights; for user and group management, for security policy changes; and for restart, shutdown, and system events. (**Note:** Because of the high volume of events that would be recorded, Windows 2000 does not normally audit the use of the Backup Files And Directories and the Restore Files And Directories rights. Appendix B, "Security In a SOFTWARE Development Environment," explains how to enable auditing of the use of these rights.) |
| Virus outbreak | Enable success and failure write access auditing for program files such as files with .exe and .dll extensions. Enable success and failure process tracking auditing. Run suspect programs and examine the security log for unexpected attempts to modify program files or creation of unexpected processes. **Note:** that these auditing settings generate a large number of event records during routine system use. You should use them only when you are actively monitoring the system log. |
| Improper access to sensitive files | Enable success and failure auditing for file- and object-access events, and then use File Manager to enable success and failure auditing of read and write access by suspect users or groups for sensitive files. |
| Improper access to printers | Enable success and failure auditing for file- and object-access events, and then use Print Manager to enable success and failure auditing of print access by suspect users or groups for the printers. |

**When should I review the auditing records?**

The administrator has to plan when designing an audit policy a set time to review the audit logs. Remember that simply auditing an event doesn't mean the system will alert you to the event--it's still up to you to read the audit logs and to determine when an event that appears in the logs represents a security breach or an attempted security breach. The frequency with which you review your audit logs should depend on the size of your organization and how big a target you are. According to AR 25-2 paragraph 4-5g, review logs and audit trails at a minimum weekly, more frequently if required and take appropriate action.

It is important that the size of the security log be configured appropriately, based on the number of events that your auditing policy settings generate. By default, the maximum size that the security event log can reach before the overwrite behavior is initiated is 512 KB. Because hard disk space is more readily available now than in the past, you will likely want to increase this setting. How much you increase this setting depends on your overwrite behavior, but a general guideline is to set the maximum size to at least 50 MB. The maximum size that you should set an event log to is 300 MB. Each security event is 350–500 bytes, so a 10-MB event log will contain approximately 20,000–25,000 security events.

You can change the maximum size of the log file on individual computers in the security event log Properties dialog box or by editing the registry. You can also change the maximum log file size on many computers by using Group Policy security templates. The maximum size for the security event log is stored in the registry value HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ Eventlog\Security\MaxSize.

When configuring the security event log settings, you must define what will happen when the maximum log file size is reached—also known as the overwrite behavior.

Windows 2000, XP, and 2003 have three overwrite behavior settings:

- Overwrite Events As Needed

  New events will continue to be written when the log is full. Each new event replaces the oldest event in the log.

- Overwrite Events Older Than [x] Days

  Retain events in the log for the number of days you specify before overwriting events. The default is 7 days.

- Do Not Overwrite Events

New events will not be recorded, and the event log will need to be cleared manually.

In addition, you can configure the OS to shut down if security events cannot be written to the security audit log file. When this setting is enabled and events cannot be written to the security event log, the computer will initiate a stop error, commonly known as the Blue Screen of Death, with the following error message:

STOP: C0000244 {Audit Failed}
An attempt to generate a security audit failed

After this stop error has occurred, only members of the local Administrators group will be allowed to log on, to troubleshoot why the events cannot be written to the event log. Until events can be written to the event log, the computer will not operate normally. This is an important setting for high-security environments because it ensures that all security events are recorded. However, a large number of security events generated by an attacker or network problem could cause a denial-of-service condition. Similarly, shutting down the server might not necessarily be in accordance with availability service level agreements (SLAs). If your organization has high security needs and high availability needs, you should implement a method of removing auditing events from the system programmatically. You can configure Windows 2000, XP, and 2003 to shut down if security events cannot be logged, by setting the registry value HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\ CrashOnAuditFail to 1.

The security event log is stored in the %systemroot%\system32\ Config\ directory in a file named SecEventevt. In Windows XP, you can change the log file location in the Properties dialog box. In Windows 2000 and 2003, you must edit the registry to change the storage location of each log file. The path and file name for the security log is stored in the registry value: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Securi ty.

By default, only the system account and the administrators group have access to the security event log to ensure that non-administrators do not have access to read, write, or delete security events. If you move the log to a new location, ensure that the new file has the correct NTFS file system permissions. Because the Event Log service cannot be stopped, changes to this setting will not take place until after the server is rebooted.  Unless you have a centralized auditing system, such as the Microsoft Operations Manager or the Microsoft Auditing Control System, you will need to carefully evaluate which overwrite behavior settings are best for your organization. In accordance with AR 25-2 para 4-5g, use audit servers to consolidate system audit logs for centralized review to remove the potential for unauthorized editing or deletion of audit logs in the event of an incident or compromise.  In general, you will want to ensure that the

security event log size is large enough to record all events that occur between the archival of events. Windows independently does not support or allow an administrator to perform this function. Third party software (i.e. Tivoli) is needed to centralize and consolidate audit logs to a separate machine and location.

**Why should I keep auditing records and how long should I keep them?**

In accordance with AR 25-2 paragraph 4-5g, administrators must maintain audit trails in sufficient detail to reconstruct events in determining the causes of compromise and magnitude of damage should a malfunction or a security violation occur. How long you keep the audit logs will depend on the kind of environment you are working in. In a low security setting, you may elect to keep the logs only for, say, the last six months. In a high security environment, you may decide to keep them permanently. Though it is tempting to make a paper record of your audit logs, it is probably more practical to keep them electronically, and then to make sure that you have backups of the logs. IAW AR 25-2 paragraph 4-5g, administrators will retain classified and sensitive information systems audit files for 1 year (5 years for SCI systems, depending on storage capability). Army Computer Emergency Response Team (ACERT), Army Network Operations and Security Center (ANOSC), Law Enforcement (LE), or Counterintelligence (CI) personnel may request information systems audit logs to support forensic investigations.

**How do you audit?**

Creating an effective audit policy is a fine balancing act between auditing enough events to be effective, but not so many events that the ones that really matter get lost. So, you have to carefully plan your audit policy. All Windows platforms have System, Application, and Security Event Logs. Depending on the server functionality, it may have three additional logs: Directory Service, DNS Server, and File Replication Service. Without proper auditing techniques, you'll never know if your security plan is working effectively. General categories to consider when setting up a secure server auditing policy are Account Logon Events, Account Management, Directory Service Access, Logon Events, Object Access, Audit Policy Changes, Use of Privileges, Process Tracking, and System Events.

1) **Enabling Auditing**
   a) To activate auditing on a standalone machine, follow these steps:
      i) Log on as the administrator of the local workstation
      ii) Click the **Start** button, point to **Programs**, point to **Administrative Tools**, and then click **Local Security Policy**.
      iii) In the **Local Security Settings** window's console tree, double-click **Local Polices** and then click **Audit Policy**.
      iv) Select the type of event to audit, and then, on the **Action** menu, click **Security.**
      v) Select the **Success** check box, the **Failure** check box, or **both.**
      vi) Click **OK**

This setting only affects the standalone system.  To set auditing on a domain
controller use Enabling Group Policy.  Failure to enable success/failure auditing
can cause hacking activities to go undetected.

**2) Enabling Group Policy**
    a) To enable which categories of event can be audited, you use the Group
       Policy Snap-in with the MMC.
       i) Click Start, Run, and enter MMC.
       ii) Select Add/Remove Snap-in from the Console menu
       iii) Click the add button
       iv) Find the Group Policy Snap-in from the "add Standalone Snap-in
           dialog box" then click add
       v) Accept the default (local computer) for where the Group Policy Object
          will be stored and click the finish button.

Failure to enable success/failure auditing can cause hacking activities to go
undetected.  Group policies may be set at the local, site, domain and
organizational unit levels.

**3) Setting up Group Policy on a Domain Controller**
    a) To set up an Audit Policy on a DC
       i) Start Menu->Admintools->AD users and Computers
       ii) Access the Group Policy properties page for the Domain Controllers
          OU.
       iii) Edit the Default Domain Controllers Policy GPO
       iv) Expand the computer configuration object in the tree window
       v) Expand the windows settings object
       vi) Expand the security settings object
       vii) Expand the local policies object and select audit policy
       viii) Double-click any policy to enable it
       ix) Check the box "define these policy settings"
       x) Check either success, failure, or both
       xi) Click "ok"
       xii) Close/Minimize windows as required
Failure to enable success/failure auditing can cause hacking activities to go
undetected.

**4) Event Log Configuration**
    a) Open the Computer Management Console
       i) Right-click  the "my computer" icon on the desktop
       ii) Select manage from the drop down menu
       iii) Expand System Tools
       iv) Expand event Viewer
       v) Right-click the event log. Perform the following procedure for each
          event log

    vi) Select properties from the pop up menu
    vii) Review the fields identifying the maximum log size and the event log
        overwriting

By default, the logs are sized as appropriated for the type of system you are
working with and its configuration.  In a standard configuration of Windows 2000,
XP, and 2003, most logs have a maximum size of 16MB.  This includes the DNS
Server, System, and Application logs.  Because they are less critical, the
Directory Service and File Replication Service logs on domain controllers have a
maximum size of 512KB.  Because the Security log is so important, it is usually
configured with a maximum size of 128 MB.  This is to allow the server to record
a complete security audit trail for situations in which the server is under attack
and a large number of security events are generated.

**5) Halt on Audit Failure**
  a) Configure the system to halt after any of the 3 logs (Application, Security,
     or System) reaches maximum size.
     i)   Start>programs>admin tools>active directory users and computers
     ii)  Right click domain controller>properties>group policy>highlight default
        policy and choose edit
     iii) Select computer configuration>windows settings>security
        settings>local policies>security options
     iv) Right click on "shut down system if unable to log security audits"
     v)  Select security>define this policy setting
     vi) Select enable
     vii) Click OK
     viii)Close windows

  b) Alternative method via the registry
     i)   Registry Hive: HKEY_LOCAL_MACHINE
     ii)  SubKey: \SYSTEM\CurrentControlSet\Control\LSA
     iii) Value Name: CrashOnAuditFail
     iv) Date Type: REG_DWORD.
     v)  The default value is 0.

The default setting is "no halt" when log files reach their maximum size.  Any log
able activities which occur after a log file has reached its maximum size, may not
be recorded.

**6) Restrict Guest Access to the Application Event Log**
  a) Restrict access to Application log
     i)   Start>programs>admin tools>active directory users and computers
     ii)  Right click domain controller
     iii) Select properties>group policy>highlight default policy and choose edit
     iv) Select computer configuration>windows settings>security
        settings>event log>settings for event logs

      v)  Right click "restrict guest access to application log"
      vi) Select security>define this policy setting
      vii) Select enable
      viii)Click OK
      ix) Close windows

   b)  Alternative method via the Registry entry:
      i)   Registry Hive: HKEY_LOCAL_MACHINE
      ii)  SubKey: \SYSTEM\CurrentControlSet\Services\Eventlog\Application
      iii) Value Name: RestrictGuestAccess
      iv) Date Type: REG_DWORD
      v)  Value Data 0x1

By default, Windows 2000 is not configured to restrict anonymous network
access to the Application log over null-session shares.

## 7) Restrict Guest Access to the Security Event Log

   a)  Restrict access to Security log.
      i)   Start>programs>admin tools>active directory users and computers
      ii)  Right click domain controller
      iii) Select properties>group policy>highlight default policy and choose edit
      iv) Select computer configuration>windows settings>security
          settings>event log>settings for event logs
      v)  Right click "restrict guest access to security log"
      vi) Select security>define this policy setting
      vii) Select enable
      viii)Click OK
      ix) Close windows

   b)  Alternative method via the Registry entry
      i)   Registry Hive: HKEY_LOCAL_MACHINE
      ii)  SubKey: \SYSTEM\CurrentControlSet\Services\Eventlog\Security
      iii) Value Name: RestrictGuestAccess
      iv) Date Type: REG_DWORD
      v)  Value Data 0x1

On a default system this key needs to be added. By default, Windows 2000 is not
configured to restrict anonymous network access to the Security log over null-
session shares.  Access to the Security Event Log is restricted to members of the
"auditors" group or other restricted membership group that serves this purpose.

## 8) Restrict Guest Access to the System Event Log

   a)  Restrict access to Security log.
      i)   Start>programs>admin tools>active directory users and computers
      ii)  Right click domain controller
      iii) Select properties>group policy>highlight default policy and choose edit

      iv) Select computer configuration>windows settings>security
          settings>event log>settings for event logs
      v) Right click "restrict guest access to system log"
      vi) Select security>define this policy setting
      vii) Select enable
      viii)Click OK
      ix) Close windows

  b) Alternative method via the Registry entry
      i) Registry Hive: HKEY_LOCAL_MACHINE
      ii) SubKey: \SYSTEM\CurrentControlSet\Services\Eventlog\System
      iii) Value Name: RestrictGuestAccess
      iv) Date Type: REG_DWORD
      v) Value Data 0x1

On a default system this key needs to be added.  By default, Windows 2000 is
not configured to restrict anonymous network access to the System log over null-
session shares.

**9)  Enable Auditing of Use of Backup Right**
  a) Configure the system to audit the user performing system backups.
      i) Start>programs>admin tools>active directory users and computers
      ii) Right click domain controller
      iii) Select properties>group policy>highlight default policy and choose edit
      iv) Select computer configuration>windows settings>security
          settings>local policies>security options
      v) Right click on "audit use of backup and restore privilege"
      vi) Select security>define this policy setting>
      vii) Select enable
      viii)Click OK
      ix) Close windows

  b) Alternative method via the Registry entry:
      i) Registry Hive: HKEY_LOCAL_MACHINE
      ii) SubKey: \SYSTEM\CurrentControlSet\Control\Lsa
      iii) Value Name: FullPrivilegeAuditing
      iv) Date Type: REG_BINARY
      v) Value Data 0x1

The default value is 0.  Unauthorized users can use the backup right to copy
sensitive system information to removable media.  Backup Operator needs to
have a unique userid dedicated for backing up the system.

**10) Auditing Printer Events**
  a) Click Start, Settings, Printers.
      i) Right-click the printer you want to manage and select properties

      ii)  Select the Security Tab.
      iii) Click the advanced button.  When the Access Control Settings window appears, select the auditing tab.
      iv) Select the add button to add an auditing record for this printer.
      v)  Select the users to which the audit record will apply.
      vi) Choose the events to audit by selecting or clearing the appropriate check boxes under the Successful or Failed columns.
      vii) Click OK when finished

**11) Setting up Events to Audit for Files and Folders**
   a) Click Start, Programs, Accessories, Windows Explorer
   b) Find the folder or file you want to set up auditing for and right-click it.
   c) Select the Security Tab from the properties box.
   d) Select the advanced button.
   e) Click the auditing tab on the Access Control Settings dialog box.
   f)  Click the add button.
   g) Select the user, computer, or group to audit
   h) Chose the appropriate check box for each type of event you want to audit on this object for the user selected
   i)  Click OK and exit all windows

# Well Known Event ID's

Common Logon Events

| Event ID | Description |
| --- | --- |
| 528 | A user successfully logged on to a computer. |
| 529 | The logon attempt was made with an unknown user name or a known user name with a bad password. |
| 530 | The user account tried to log on outside the allowed time. |
| 531 | A logon attempt was made by using a disabled account. |
| 532 | A logon attempt was made by using an expired account. |
| 533 | The user is not allowed to log on at this computer. |
| 534 | The user attempted to log on with a logon type that is not allowed, such as network, interactive, batch, service, or remote interactive. |
| 535 | The password for the specified account has expired. |
| 536 | The Netlogon service is not active. |
| 537 | The logon attempt failed for other reasons. |
| 538 | A user logged off. |
| 539 | The account was locked out at the time the logon attempt was made. This event is logged when a user or computer attempts to authenticate with an |

## Common Logon Events

| Event ID | Description |
| --- | --- |
| | account that has been previously locked out. |
| 540 | Network logon succeeded. |
| 682 | A user has reconnected to a disconnected Terminal Services session. |
| 683 | A user disconnected a Terminal Services session without logging off. |

## Common Object Access Events

| Event ID | Description |
| --- | --- |
| 560 | Access was granted to an already existing object. |
| 561 | A handle to an object was allocated. |
| 562 | A handle to an object was closed. |
| 563 | An attempt was made to open an object with the intent to delete it. |
| 564 | A protected object was deleted. |
| 565 | Access was granted to an already existing object type. |

## Common Policy Change Events

| Event ID | Description |
| --- | --- |
| 608 | A user right was assigned. |
| 609 | A user right was removed. |
| 610 | A trust relationship with another domain was created. |
| 611 | A trust relationship with another domain was removed. |
| 612 | An audit policy was changed. |
| 671 | Security policy was changed or refreshed. ("--" in the Changes Made field means that no changes were made during the refresh.) |
| 768 | A collision was detected between a namespace element in one forest and a namespace element in another forest. |

## Common Privilege Use Events

| Event ID | Description |
| --- | --- |
| 576 | Specified privileges were added to a user's access token. (This event is generated when the user logs on.) |
| 577 | A user attempted to perform a privileged system service operation. |
| 578 | Privileges were used on an already open handle to a protected object. |

Common System Events

| Event ID | Description |
| --- | --- |
| 512 | Windows is starting up. |
| 513 | Windows is shutting down. |
| 514 | An authentication package was loaded by the Local Security Authority (LSA). |
| 515 | A trusted logon process has registered with the LSA. |
| 516 | Internal resources allocated for the queuing of security event messages have been exhausted, leading to the loss of some security event messages. |
| 517 | The security log was cleared. |
| 518 | A notification package was loaded by the Security Accounts Manager (SAM). |

Using Microsoft website will help explain in more detail some of the events.  You may also reference the website **www.eventid.net.**

## Section 8 – Web Server Security

If you keep track of the various security alerts that cascade through the internet you'll notice that Microsoft IIS gets plenty of mention.  IIS is probably the best known of the web server applications but it is Apache that has been the most popular web server on the Internet since April of 1996. The February 2005 Netcraft Web Server Survey found that, of the 20 million websites on the Internet, more than 68% of the web sites are using Apache, thus making it more widely used than all other web servers combined.  Microsoft's Internet Information Services (IIS) is the main competitor to Apache. Solaris Operating Environment/J2EE also competes in the enterprise web services arena.   There are almost 20 million websites world-wide.

The U.S. Army has had a long love/hate affair with IIS.  In March of 2000 Army CIO, LtGen Campbell moved the Official Army web site from Microsoft IIS 4 servers to Mac G3 servers running WebSTAR.  The Microsoft IIS 4 systems had been hacked so many times that a change was required.

By 2003 a large majority of Army web servers were running Microsoft 2000 with IIS 5.  A buffer overflow vulnerability was exposed as hackers were able to take complete control of a 2000 server and any supported website.  By sending a specially crafted request to an IIS 5.0 server, an attacker was able to execute arbitrary code in the local system security context, essentially giving the attacker compete control of the system, this according to a CERT bulletin. This is a bit more serious than a simple 'Web defacement.'  Due to security concerns the exact computer in the U.S. Army that was hacked was never revealed.  The sensitivity of the data contained on the system, and the attacker's intentions are not intended for public discourse. Surprisingly the Army unit did not have a standard operating procedure in place to execute after they found the flaw. Events of the attack also failed to properly make its way up the reporting chain.

System administrators sometimes do all the wrong things first.  What happened in this event was the Army unit first took down the affected machine and rebuilt it, which lost valuable forensic evidence and left the rebuilt computer vulnerable to another attack.  The attack was reported as a bug to a general Microsoft Web site, where it languished for a few hours before the company responded. The sysadmins then blocked the outbound port in an effort to keep the attacker from exporting data even though the hacker could have simply changed the port he or she was using or used multiple ports simultaneously.

Compounding the surprising nature of an attack on a Defense Department system is the fact that this was a previously unknown vulnerability, or "zero-day exploit," which are extremely rare in the computer security arena. Vendors often issue patches before hackers have infiltrated a system.  The hacker also left behind a file with the phrase, "Welcome to the Unicorn beachhead." Of the some

8,000 known hackers at that time, none went by the name "Unicorn". The Army has to be prepared against attacks of this nature as they may not be the work of random hackers but the work of hostile governments.

Good or bad, the U.S. Government tends to lean more towards Microsoft's IIS versions as Apache is an open source solution. Microsoft and especially IIS has long been the target of the hacker underworld. U.S. military networks are under a constant barrage of scans and intrusion attempts. It takes common sense, skill and presence of mind to keep the world out of your network while permitting them to view your web-site.

Quick web server statistic:
- --Web Server Attacks and Web Site Defacements Up Thirty-Six Percent (27/26 April 2005) A report from security firm Zone-H finds that web server attacks and web site defacements increased by 36% the last year, from 251,000 in 2003 to 392,545 in 2004. According to the report, 2,500 web servers are successfully attacked every day.

When you set up a web server you have to address the following security areas:
- Platform Security
- Web Server Security
- Communications Security
- Application Security

To help you achieve the above 4 areas of security, you need to utilize access controls.
There are four methods of access control that can be applied to servers running a web server or more specifically IIS. A user must pass through these security checks before gaining access to a specific resource.

- IP Access: Configure the Web server to prevent specific computers, groups of computers, or entire networks from accessing the WEB server.

- User Authentication: Configure the Web server to allow anonymous (guest) access or to require clients to use Windows NT logon to gain access.

- Web Permission: Configure the Web server's access permissions- READ, WRITE, or EXECUTE for specific sites, directories, and files. The permissions will apply to all users regardless of their specific access rights.

- File Security: IIS relies on NTFS permissions for securing individual files and directories from unauthorized access. Unlike Web server permissions

which apply to all users, NTFS permissions can be used to precisely define which user can access the contents and what they can do to it.

Here are some of the basic guidelines when you set up your server to perform web server duties.

- Resolve the physical, environmental, network, and security policy issues.
- Identify roles and responsibilities of the individuals involved in multi-level administration
- Learn how the hackers exploit web servers and what tools they utilize. This gives you a better chance of defending against them.
- Remove all unnecessary services, modify default account settings
- Set rules for authentication, IP filtering, network address translation, and domain restrictions
- Use Virtual Private Networks, SSL encryption and PKI effectively
- Monitor your web site activity and review your logs
- When using Active Server Pages, use only safe scripts
- Secure all related IIS services (FTP, SMTP, NNTP)

Set the NTFS File and Directory Permissions

- Create WebAdmin group and put all web administrators in the group
- Remove EVERYONE GROUP from the ACL for virtual directories or Web Pages Administrators
- Add
    o WebAdmin group with full controls
    o IUSER_*Computer* with appropriate permissions
    o Authenticated Users with appropriate permissions

Combine NTFS and IIS Permissions
- Assign permissions in IIS
    o Read permission to the directory to allow browsing.
    o Script permission for directories containing Active Server Pages, CGI or other scripts.
- Assign permissions in NTFS
    o Read permissions to the Users local groups.
    o Change permissions to group responsible for creating content in the directory.
    o Full control permission to the Web Administrators local group responsible for administrating the Web server.
    o No access permission to any group or user who should not be allowed to browse the contents of the directory.

Secure Sockets Layer (SSL)
- Supports web browsers and servers
- Uses a one way public key algorithm (by default).
- Server issues its public key.
- Client generates a session key using browser.
- Client sends session key to Server encrypted with Server public key.
- Client and Server exchange information using session key generated by client.
- Can you be sure that the Server is who he says he is?
- The standard case does not authenticate client.

Secure Sockets Layer (SSL) allows a client and server to encrypt all data being transferred between them.  The SSL protocol is built into all current web browsers, and requires a web server to obtain a Server Certificate that can be authenticated by a web client through a third party Certificate Authority.  The Server Certificate acts as a digital signature and allows the client to confirm that the server's identity is authentic.

The SSL Authentication process is as follows:
1. The client WEB browser requests a secure communication link from the web server (via an https://server request).

2. The web server sends the browser a copy of it's Certificate along with it Public Key.  The certificate enables the browser to confirm the server's identify and the integrity of the Web content.

3. The WEB browser sends a "Session Key" to the web server, encrypted with the server's public key.  The browser then sends the encrypted session key to the web server.

4. Using its own private key, the server decrypts the session key and establishes a secure channel.

5. The browser and server each use the Session Key to encrypt and decrypt all further traffic between the client and server.

Web Server Vulnerabilities
- CGI Scripts
  - CGIs (Common Gateway Interfaces) CGI are scripts written in Perl, batch file, c++ or numerous languages that interfaces between the Web server and the web page.  When you click on a button on a web page the script is what tells the server what action to perform next.
- Active Server Pages (*ASP*)
- Server Side Includes
- Superfluous Decoding Operation

- Buffer Overflows
- Security Policies
- Administrators
- Denial of Service attacks
  - One of the government's biggest fears is that the hackers will be able to shut down any webserver at any given time.  These are just a few types of DOS attacks.
    - Bandwidth Consumption
    - Resource Starvation
    - DNS Attacks
    - Malformed  URL
    - Malformed WebDAV Request

Some of the major IIS 6.0 new security features include:

- Locked down Web environment by default
  In order to reduce the attack surface of systems, IIS 6.0 is not installed by default on Windows Server 2003 — administrators must explicitly select and install it.
- Automatically rejects files with unknown file extensions
  The default installation of IIS will not compile, execute, or serve files with dynamic extensions. In order to be served, each acceptable file extension must be added to the Web service extension list.
- Default low-privilege account
  All IIS 6.0 worker processes run with fewer, more limited operating system privileges on Windows Server 2003 by default.
- Fault-tolerant process architecture
  IIS 6.0 isolates Web sites and applications into self-contained units, called application pools, so that errors in one application pool can't cause another application pool or the server itself to fail.
- Buffer and memory-overflow protection
  This feature provides protection against the most common types of Web attacks by ensuring that once a buffer or memory overflow has been detected in a particular worker process, the worker process is shut down so that it can't affect other worker processes.

Microsoft Technet is the stop source for IIS security information:

- http://www.microsoft.com/technet/security/prodtech/IIs.mspx

**Section 9 – Securing Methods**

**Securing Services**

By default, services are started under the LocalSystem account in Windows 2000.  The LocalSystem account has unlimited access not only to the service, but also to the server itself.  If compromised, an intruder can insert malicious code that will be executed during or upon completion of the service.  The code can be anything from installing a Trojan on the server to altering/deleting system files.

Windows Server 2003 includes three built – in local accounts that are used as the logon accounts for various system services:

**Local System account:** The Local System account is a powerful account that has full access to the system and acts as the computer on the network. If a service logs on to the Local System account on a domain controller, that service has access to the entire domain. Some services are configured by default to log on to the Local System account. Do not change the default service setting. The name of the account is LocalSystem. This account does not have a password.

**Local Service account:** The Local Service account is a special, built – in account that is similar to an authenticated user account. The Local Service account has the same level of access to resources and objects as members of the Users group.  This limited access helps safeguard your system if individual services or processes are compromised. Services that run as the Local Service account access network resources as a null session with anonymous credentials. The name of the account is NT AUTHORITY\LocalService. This account does not have a password.

**Network Service account:** The Network Service account is a special, built – in account that is similar to an authenticated user account. The Network Service account has the same level of access to resources and objects as members of the Users group. This limited access helps safeguard your system if individual services or processes are compromised. Services that run as the Network Service account access network resources using the credentials of the computer account. The name of the account is NT AUTHORITY\NetworkService. This account does not have a password.

Any service or application is a potential point of attack. It is recommended that you disable or remove any unneeded services or executable files in your system environment. It is important that you know what services are required for your system to perform its essential tasks.

To utilize the Services Snap-in within the Microsoft Management Console (MMC) to start and stop services.  This tool can be used both locally and remotely:

- Click the **Start** button and choose **Run**.
- Type in **MMC**.
- Once the MMC console box comes up left-click on **Console** from the tool bar.
- Choose **Add/Remove Snap-in**.
- Left-click **Add**, choose **Services**, left-click **Add, Close, OK**.
- Expand the Services policy.
- Choose the Services to stop.
- Save the policy to the default directory and reboot the server.
- From here you can double-click on the services that you wish to modify.

The Services snap-in is the preferred method to manage your services.  It provides a central point of management.  If the service is not needed, stop it.  Other ways of getting to the services snap-in is to go Start-Programs-Administrator Tools-Services or type services.msc at the command prompt, run command or utilize the command line tool **net.exe**.

To utilize the command line tool **net.exe**.  It exposes basic start/stop/pause and query functionality.

- From the command line, type **net.exe** to view the available syntax
- To stop a service, type **net stop** *service*. (service being the name of the service you wish to stop)
- To start a service, type **net start** *service*.  Without a parameter, this command will provide a list of started services.
- To pause a service, type **net pause** *service*.
- To continue a service from a pause, type **net continue** *service.*

Services can
- Automatically start each time a computer starts.
- Run when no user is logged on to the computer.  In fact, services can run even if no user is ever logs on to the computer.
- Respond to requests without human intervention.
- Be configured to automatically restart if it fails.

From the services snap-in one can
- Configure the startup behavior for each service.
- Stop, start, pause, and resume services.
- Configure the security context under which the service runs.

Startup Values for Services

| Startup Value | Registry Value | Description |
|---|---|---|
| Boot Start | 0x0 | Ntldr or Osloader preloads the driver so that it is in memory during system boot. This value is used only for kernel-mode drivers, which are generally not manageable by administrators. This value can be set only in the registry. |
| System Start | 0x1 | The driver loads and initializes after Boot Start drivers have initialized. The Boot Start drivers are loaded before the Starting Windows screen appears. This value can be set only in the registry. |
| Automatic | 0x2 | The SCM starts services with an automatic startup value during the boot process when the Starting Windows screen appears. The progress bar indicates the loading and starting of services. Some services are not loaded until after the network devices have been initialized. |
| Manual | 0x3 | The SCM starts the service when prompted by another application or a user with the necessary permissions. Often services will start dependant services only when they are needed. |
| Disabled | 0x4 | The SCM will not permit the service to be started. |

## Windows 2000 Default services

| Service | Full Name | Default |
|---|---|---|
| Alerter | Alerter | Automatic |
| AppMgmt | Application Management | Manual |
| ClipSrv | ClipBook | Manual |
| EventSystem | COM+ Event System | Manual |
| Browser | Computer Browser | Automatic |
| DHCP | DHCP Client | Automatic |
| Dfs | Distributed File System | Automatic |
| TrkWks | Distributed Link Tracking Client | Automatic |
| TrkSrv | Distributed Link Tracking Server | Manual |
| MSDTC | Distributed Transaction Coordinator | Automatic |
| DNSCache | DNS Client | Automatic |
| EventLog | Event Log | Automatic |
| Fax | Fax Service | Manual |
| NtFrs | File Replication | Manual |
| IISADMIN | IIS Admin Service | Automatic |
| Cisvc | Indexing Service | Manual |

| | | |
|---|---|---|
| SharedAccess | Internet Connection Sharing | Manual |
| IsmServ | Intersite Messaging | Disabled |
| PolicyAgent | IPSEC Policy Agent(IPSEC Service) | Automatic |
| Kdc | Kerberos Key Distribution Center | Disabled |
| LicenseService | License Logging Service | Automatic |
| Dmserver | Logical Disk Manage | Automatic |
| Dmadmin | Logical Disk Manager Administrative Service | Manual |
| Messenger | Messenger | Automatic |
| Netlogon | Net Logon | Automatic* |
| Mnmsrvc | NetMeeting Remote Desktop Sharing | Manual |
| Netman | Network Connections | Manual |
| NetDDE | Network DDE | Manual |
| NetDDEdsdm | Network DDE DSDM | Manual |
| NtLmSsp | NTLM Security Support Provider | Manual |
| SysmonLog | Performance Logs and Alerts | Manual |
| PlugPLay | Plug and Play | Automatic |
| Spooler | Print Spooler | Automatic |
| ProtectedStorage | Protected Storage | Automatic |
| RSVP | QoS Admission Control (RSVP) | Manual |
| RasAuto | Remote Access Auto Connection Manager | Manual |
| RasMan | Remote Access Connection Manager | Manual |
| RpcSs | Remote Procedure Call (RPC) | Automatic |
| Rpclocator | Remote Procedure Call (RPC) Locator | Manual |
| RemoteRegistry | Remote Registry Service | Automatic |
| NtmsSvc | Removable Storage | Automatic |
| RemoteAccess | Routing and Remote Access | Disabled |
| Seclogon | RunAs Service | Automatic |
| SamSs | Security Accounts Manager | Automatic |
| Lanmanserver | Server | Automatic |
| SMTPSVC | Simple Mail Transport Protocol (SMTP) | Automatic |
| ScardSvr | Smart Card | Manual |
| ScardDrv | Smart Card Helper | Manual |
| SENS | System Event Notification | Automatic |
| Schedule | Task Scheduler | Automatic |
| LmHosts | TCP/IP NetBIOS Helper Service | Automatic |
| TapiSrv | Telephony | Manual |
| TlntSvr | Telnet | Manual |
| TermService | Terminal Services | Disabled |
| UPS | Uninterruptible Power Supply | Manual |
| UtilMan | Utility Manager | Manual |
| MSIServer | Windows Installer | Manual |
| WinMgmt | Windows Management Instrumentation | Manual |

| WMI | Windows Management Instrumentation Driver Extensions | Manual |
|---|---|---|
| W32Time | Windows Time | Automatic* |
| LanmanWorkstation | WorkStation | Automatic |
| W3svc | World Wide Web Publishing Service | Automatic |

**Windows Server 2003** has Local Service and Network Service groups and uses them, rather than the more-privileged local system, to run certain services. These are enumerated below:

**Services that run under Local Service**
Alerter
Application layer gateway service
Remote Registry
Smart Card
Smart Card Helper
SSDP Discovery Service
TCP/IP NetBIOS Helper
Telnet
UPS
Universal Plug and Play
Web Client
Windows Image Acquisition
WinHTTP Web Proxy Auto-Discovery Service

**Services that run under Network Service**
DHCP Client
Distributed Transaction Coordinator
DNS Client
License Logging
Performance Logs and Alerts
RPC Locator

In Windows Server 2003 member servers, the Kerberos KDC service is disabled by default and then automatically enabled through dcpromo. Internet Information Services (IIS) is not installed by default, and when it is installed, the default behavior is only to display static pages.

In addition, Windows Server 2003 disables the following services by default:
Alerter
Clipbook
Distributed Link Tracking Server
Human Interface Device Access
Imapi CDROM Burning Service
ICF\ICS
Intersite Messaging
License Logging

Messenger
NetMeeting Remote Desktop Sharing
Network DDE
Network DDE DSDM
Routing and Remote Access
Telnet
Terminal Service Session Discovery
Themes
WebClient
Windows Image Acquisition (WIA)

## TCP/IP

TCP/IP is an open protocol created to connect heterogeneous computing environments with the least amount of overhead possible. As is often the case, interoperability and performance design goals do not generally result in security—and TCP/IP is no exception to this. TCP/IP provides no native mechanism for the confidentiality or integrity of packets. To secure TCP/IP, you can implement IP Security. IPSec implements encryption and authenticity at a lower level in the TCP/IP stack than application-layer protocols such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS). Because the protection process takes place lower in the TCP/IP stack, IPSec protection is transparent to applications. IPSec is a well-defined, standards-driven technology. The two core protocols of the transport layer are transmission control protocol (TCP) and user datagram protocol (UDP).

There are numerous threats to TCP/IP that can compromise network security or lead to information disclosure.  Some of the common threats include port scanning, spoofing and denial of service.  Windows 2000/XP/2003 include support for TCP/IP filtering.  TCP/IP filtering allows you to specify which types of inbound local host IP traffic are processed for all interfaces.  This feature prevents traffic from being processed by the computer in the absence of the other TCP/IP filtering.  TCP/IP filtering by default is disabled in Windows 2000/XP/2003.

### How to configure TCP/IP security

To configure TCP/IP security:

1. Click **Start** , point to **Settings** , click **Control Panel** , and then double-click **Network Connections** .

2. Right-click the interface on which you want to configure inbound access control, and then click **Properties** .

3. In the **Components checked are used by this connection** box, click **Internet Protocol (TCP/IP)** , and then click **Properties** .

4. In the **Internet Protocol (TCP/IP) Properties** dialog box, click **Advanced** .

5. Click the **Options** tab.

6. Click **TCP/IP filtering** , and then click **Properties** .

7. Select the **Enable TCP/IP Filtering (All adapters)** check box. When you select this check box, you enable filtering for all adapters, but you configure the filters on a per-adapter basis. The same filters do not apply to all adapters.

8. There are three columns with the following labels:

   **TCP Ports**
   **UDP Ports**
   **IP Protocols**

   In each column, you must select either of the following options:

   **Permit All** . If you want to permit all packets for TCP or UDP traffic, leave **Permit All** activated.

   **Permit Only** . If you want to allow only selected TCP or UDP traffic, click **Permit Only** , click **Add** , and then type the appropriate port in the **Add Filter** dialog box.

   If you want to block all UDP or TCP traffic, click **Permit Only** , but do not add any port numbers in the **UDP Ports** or **TCP Port** column. You cannot block UDP or TCP traffic by selecting **Permit Only** for **IP Protocols** and excluding IP protocols 6 and 17.

   Note that you cannot block ICMP messages, even if you select **Permit Only** in the **IP Protocols** column and you do not include IP protocol 1.

TCP/IP Filtering can filter only inbound traffic. This feature does not affect outbound traffic or response ports that are created to accept responses from outbound requests.

One of the biggest security issues on a network is network traffic passed along the wire as unencrypted, or clear-text, data.  When your information is traveling

as clear-text (as most SMTP, Telnet, HTTP, and FTP traffic does), an attacker who has gained access to your physical network can listen in and read any unencrypted traffic.  By allowing unencrypted traffic on your network, you are vulnerable to many different attacks such as, network sniffing, Man-in-the-Middle, and spoofing just to name a few. How can we actually see this?  What can we do to prevent this?

**Network Monitor**

Network Monitor is a component of the Windows Server OSs and Microsoft Systems Management Server (SMS) that lets you monitor network traffic as it crosses the wire. By using Network Monitor, you can monitor network traffic in real time or capture and store packets for later analysis. You can use the information that Network Monitor captures to troubleshoot problems on LANs, WANs, and virtually any device that uses TCP/IP to communicate. Network Monitor has many uses:

- **Troubleshooting network connectivity**. This is the number-one reason to use Network Monitor. If you have two machines that have problems communicating with each other, you can use Network Monitor's Network Trace feature to help determine the problem's exact cause. You can also use Network Monitor to view each TCP/IP packet that travels between the two devices and the information contained within each packet.
- **Assessing network performance.** Network Monitor gives you a clear picture of current network utilization. If you suspect that you have a network performance bottleneck, you can use the information that Network Monitor provides—such as detailed network-utilization statistics and information about the network traffic source—to find the bottleneck. Although you typically won't use Network Monitor to initially identify a problem as network communications related, it's a great second-level troubleshooting tool that can help you further pinpoint a problem and displays much more detail than Performance Monitor does.

**IPSEC**

**What is IPSEC?**
- IP Security is a set of protocols and standards to support the securing of data at the IP layer.  IPSec is a framework, not an implementation.
- Supports authentication and encryption of traffic.
  - Certifies the originator of the packet.
  - Protects the data from interception and tampering while in transit.

**Why do we want to use IPSec?**
- Secure our network
- Transparent operation

- IPSec allows us to secure any IP based protocol transparent to the application.
- Support for legacy software which is inherently insecure (telnet,ftp,SMB).
- An alternative mechanism to implementing application level security such as using SSL.

**Choosing Between IPSec Modes**

IPSec operates in two modes: transport mode and tunnel mode. IPSec transport mode is used for host-to-host connections, and IPSec tunnel mode is used for network-to-network or host-to-network connections.

**Using IPSec Transport Mode**

IPSec transport mode is fully routable, as long as the connection does not cross a network address translation (NAT) interface, which would invalidate the ICV. Used this way, IPSec must be supported on both hosts, and each host must support the same authentication protocols and have compatible IPSec filters configured and assigned. IPSec transport mode is used to secure traffic from clients to hosts for connections where sensitive data is passed.

**Using IPSec Tunnel Mode**

IPSec tunnel mode is used for network-to-network connections (IPSec tunnels between routers) or host-to-network connections (IPSec tunnels between a host and a router). Used this way, IPSec must be supported on both endpoints, and each endpoint must support the same authentication protocols and have compatible IPSec filters configured and assigned. IPSec tunnel mode is commonly used for site-to-site connections that cross public networks, such as the Internet.

**IPSec Modes**
- Transport – Secures the payload part of the IP packet, leaves the IP header unsecured.  Commonly use for securing traffic on a LAN. (Host to Host)
- Tunnel – Secures the entire IP packet and encapsulates it within a new IP packet.  Commonly used for creating a VPN. (Network to Network or Host to  Network)

IPSec is comprised of two protocols: IPSec Authentication Header (AH) and IPSec Encapsulating Security Payload (ESP). Each protocol provides different services; AH primarily provides packet integrity services, while ESP provides packet confidentiality services. IPSec provides mutual authentication services between clients and hosts, regardless of whether AH or ESP is being used.

IPSec AH provides authentication, integrity, and anti-replay protection for the entire packet, including the IP header and the payload. AH does not provide confidentiality. When packets are secured with AH, the IPSec driver computes an Integrity Check Value (ICV) after the packet has been constructed but before it is sent to the computer.

The IPSec process encrypts the payload after it leaves the application at the client and then decrypts the payload before it reaches the application at the server. An application does not have to be IPSec aware because the data transferred between the client and the server is normally transmitted in plaintext.

**IPSec protocols – AH protocol**

AH - Authentication Header

- Defined in Request for Comment (RFC) 1826
- Integrity: Yes, including IP header
- Authentication: Yes
- Non-repudiation: Depends on cryptography algorithm.
- Encryption: No
- Replay Protection: Yes

ESP packets are used to provide encryption services to transmitted data. In addition, ESP provides authentication, integrity, and anti-replay services. When packets are sent using ESP, the payload of the packet is encrypted and authenticated.

**IPSec protocols – ESP protocol**

ESP – Encapsulating Security Payload

- Defined in RFC 1827
- Integrity: Yes
- Authentication: Depends on cryptography algorithm.
- Non-repudiation: No
- Encryption: Yes
- Replay Protection: Yes

**Differences between AH and ESP**:

- ESP provides encryption, AH does not.
- AH provides integrity of the IP header, ESP does not.
- AH can provide non-repudiation.  ESP does not.
- However, we don't have to choose since both protocols can be used in together.

**Why have two protocols?**

- Some countries have strict laws on encryption. If you can't use encryption in those countries, AH still provides good security mechanisms. Two protocols ensures wide acceptance of IPSec on the Internet.

**Selecting an IPSec Authentication Method**

During the initial construction of the IPSec session—also known as the Internet Key Exchange, or IKE—each host or endpoint authenticates the other host or endpoint. When configuring IPSec, you must ensure that each host or endpoint supports the same authentication methods. IPSec supports three authentication methods:

- Kerberos
- X.509 certificates
- Preshared key

**Authenticating with Kerberos**

In Windows 2000 and Windows XP, Kerberos is used for the IPSec mutual authentication by default. For Kerberos to be used as the authentication protocol, both hosts or endpoints must receive Kerberos tickets from the same Active Directory directory service forest. Thus, you should choose Kerberos for IPSec authentication only when both hosts or endpoints are within you own organization. Kerberos is an excellent authentication method for IPSec because it requires no additional configuration or network infrastructure.

**Authenticating with X.509 Certificates**

You can use X.509 certificates for IPSec mutual authentication of hosts or endpoints. Certificates allow you to create IPSec secured sessions with hosts or endpoints outside your Active Directory forests, such as business partners in extranet scenarios. You also must use certificates when using IPSec to secure VPN connections made by using Layer Two Tunneling Protocol (L2TP). To use certificates, the hosts must be able to validate that the other's certificate is valid.

**Authenticating with Preshared Key**

You can use a preshared key, which is a simple, case-sensitive text string, to authenticate hosts or endpoints. Preshared key authentication should be used only when testing or troubleshooting IPSec connectivity because the preshared key is not stored in a secure fashion by hosts or endpoints.

**Creating IPSec Policies**

IPSec is a policy-driven technology. In Windows 2000 and Windows XP, you can have only one IPSec policy assigned at a time. IPSec policies are dynamic, meaning that you do not have to stop and start the IPSec service or restart the computer when assigning or unassigning IPSec policies. You can also use Group Policy to deploy IPSec policies to Windows 2000 and Windows XP clients. Windows 2000 and Windows XP include three precreated IPSec policies:

- **Client** (Respond Only)

  A computer configured with the Client policy will use IPSec if the host it is communicating with requests using IPSec and supports Kerberos authentication.

- **Server** (Request Security)

  A computer configured with the Server policy will always attempt to negotiate IPSec but will permit unsecured communication with hosts that do not support IPSec. The Server policy permits unsecured ICMP traffic.

- **Secure Server** (Require Security)

  A computer configured with the Secure Server policy will request that IPSec be used for all inbound and outbound connections. The computer will accept unencrypted packets but will always respond by using IPSec secured packets. The Secure Server policy permits unsecured ICMP traffic.

In addition to the built-in policies, you can create custom IPSec policies. When creating your own IPSec policies, you must configure rules that include the following settings:

- IP Filter List
- Tunnel Settings
- Filter Actions
- Authentication Methods
- Connection Types

**How IPSec Works**

IPSec can be initiated by either the sending host or the receiving host. The two hosts or endpoints enter into a negotiation that will determine how the communication will be protected. The negotiation is completed in the Internet Key

Exchange (IKE) and the resulting agreement is a set of security associations, or SAs.

IKE has two modes of operation, main mode and quick mode. IKE also serves two functions:

- Centralizes SA management, reducing connection time
- Generates and manages the authenticated keys used to secure the information

The SA is used until the two hosts or endpoints cease communication, even though the keys used might change. A computer can have many SAs. The SA for each packet is tracked using the Security Parameter Index (SPI).

**Main Mode**

During the main mode negotiation, the two computers establish a secure, authenticated channel—the main mode SA. IKE automatically provides the necessary identity protection during this exchange. This ensures no identity information is sent without encryption between the communicating computers, thus enabling total privacy.

**Monitoring IPSec**

You can monitor IPSec in Windows 2000 with IPSecmon.exe and in Windows XP/2003 with the IP Security Monitor Microsoft Management Console (MMC) snap-in. In addition, you can create log files in both Windows 2000 and Windows XP/2003 to view IPSec negotiations.

**Using IPSecmon in Windows 2000**

In Windows 2000, you can view the status of IPSec SAs and basic information on IPSec sessions by running IPSecmon from the Run prompt. IPSecmon displays information about each SA and the overall statistics of IPSec and IKE sessions.

**Using the IP Security Monitor MMC Snap-In (Windows XP/2003)**

In Windows XP/2003, IPSecmon has been replaced with an MMC snap-in that provides all the information that IPSecmon did in Windows 2000, only in much greater detail. You can use the IP Security Monitor MMC snap-in to view details of each SA, whereas in Windows 2000, you could view only the basic details of an SA. The IP Security Monitor MMC snap-in in Windows XP/2003 enables you to view the exact SA details negotiated during both main mode and quick mode.

**Using IPSec Logs in Windows 2000 and Windows XP/2003**

In both Windows 2000 and Windows XP/2003, you can have IPSec log the IKE exchanges to a log file on the hard drive for troubleshooting or monitoring needs. To have your computer log IKE exchanges, you must create a registry value named EnableLogging in the registry key HKLM\System\CurrentControlSet\Services\PolicyAgent\Oakley. To enable logging, set the value to 1 and restart the IPSec services. The log file will be written to the file %systemroot%\ debug\oakley.log. Ipseclog.vbs automatically configures the registry in Windows 2000 and Windows XP/2003 to enable IPSec logging.

You must be a member of the **Administrators group** to set Internet Protocol security (IPSec) policies. If the computer participates in a Windows 2000/2003 domain, the computer may receive the IPSec policy from Active Directory, overriding the local IPSec policy. In this case, the options are disabled and you cannot change them from the local computer.

Select an IPSec policy (Windows 2000)

- Open **Network and Dial-up Connections** on **Control Panel** (or right click on **Network Places** and click **Properties**).
- Click **Local Area Connection**, and on the **File** menu, click **Properties**.
- In the **Local Area Connection Properties** dialog box, under **Components checked are used by this connection**, click **Internet Protocol (TCP/IP)**, and then click **Properties**.
- Click **Advanced**, and then click the **Options** tab.
- Under **Optional settings**, click **IP security**, and then click **Properties**.
- Click **Use this IP security policy**, and then select the IPSec policy you want from the drop-down list.

An alternative method of selecting IPSEC Policy is through the MMC.

- Click the **Start** button and choose **Run**.
- Type in **MMC**.
- Once the MMC console box comes up left-click on **Console** from the tool bar.
- Choose **Add/Remove Snap-in**.
- From the Snap-in window choose **Add.**
- Choose **IP Security Policies on Active Directory.**
- Choose **Close.**
- Choose **OK.**
- Expand the policy and choose which policy best meets your requirements.
- Save the new settings under the default directory and reboot the server.

**Authentication Protocols in Windows**

Windows NT, Windows 2000 ,Windows XP and Windows 2003 support authentication using the LAN Manager (LM), NT LAN Manager (NTLM), and NT LAN Manager version 2 (NTLM2) protocols. Windows 2000/XP/2003 use Kerberos v5 as the default network authentication protocol.

Windows support these several protocols for verifying the identity of users who claim to have accounts on the system. These also include protocols for authenticating dial-up connections and protocols for authenticating external users who try to connect to the network over the Internet

**NTLM**

The NTLM protocol authenticates users and computers based on a challenge/response mechanism. When the NTLM protocol is used, a resource server must contact a domain authentication service on the domain controller for the computer or user's account domain to verify its identity whenever a new access token is needed. In the absence of a domain, the NTLM protocol can also be used for peer-to-peer authentication.

NTLM authentications in Windows 2000/XP/2003 support the following three methods of challenge/response authentication:

**LAN Manager (LM):** the **least secure form** of challenge/response authentication that is supported by Windows 2000/XP/2003, (but more secure than cleartext). LM is available so that computers running Windows 2000/XP/2003 can connect to file shares on computers running legacy OS. LM passwords are limited to 14 characters. With LM, passwords themselves are not stored by the operating system. Instead, the passwords are encrypted with the LAN Manager one-way function (OWF), which is formed by converting the password to uppercase characters, breaking the 14-character password into 7-character halves, adding padding for passwords with less than 14 characters, and encrypting a constant with the 7-character halves by using the DES encryption algorithm. There are many tools on the Internet today that will easily crack these passwords.

**NTLM version 1:** is a more secure form of challenge/response authentication than LM. It is available so that computers running Windows XP Professional can connect to servers in a Windows NT domain that has at least one domain controller running Windows NT 4.0 Service Pack 3 or earlier. NT LAN Manager,

also known as NTLM, first shipped with Windows NT and is an improvement over the LM authentication protocol. Unlike LM passwords, NTLM passwords are based on the Unicode character set, are case sensitive, and can be up to 128 characters long. As with LM, the operating system does not actually store the password; rather, it stores a representation of the password by using the NTLM OWF. The NTLM OWF is computed by using the MD4 hash function, which computes a 16-byte hash, or digest, of a variable-length string of text, which in this case is the user's password. Another difference between NTLM and LM is that NTLM passwords are not broken into smaller pieces before having their hash algorithm computed. NTLM uses the same challenge/response process for authentication as LM does. NTLM is the default authentication provider in Windows NT and Windows 2000 (when the Windows 2000 machine is not a member of an Active Directory domain).

**NTLM version 2:** the most secure form of this type of challenge/response authentication that is supported by Windows XP Professional. It is used when computers running Windows XP Professional connect to servers in a Windows NT domain where all domain controllers are upgraded to Windows NT 4.0 Service Pack 4 or later. It is also used when computers running Windows 2000 or Windows XP Professional connect to servers running Windows NT in a Windows 2000 domain. In addition, computers running Windows 95 or Windows 98 can use this form of challenge/response authentication if the Directory Service Client Pack has been installed.

By default, all three challenge/response mechanisms are enabled so that clients running Microsoft Windows for Workgroups, Windows 95, or Windows 98 (legacy OS) can access network resources. You can disable authentication that uses weaker variants by setting the LAN Manager authentication level security option in Local Security Policy\Computer Configuration\Windows Settings\Local Policies\Security Options or in the appropriate security template. If you do so, however, computers that rely on the weaker variants for authentication might not be able to access network resources.

**Kerberos V5 Authentication Protocol**

The Kerberos V5 protocol provides a means for mutual authentication between a client, such as a user, computer, or service, and a server. This is a more efficient means for servers to authenticate clients, even in the largest and most complex network environments. The Kerberos protocol is based on the assumption that initial transactions between clients and servers take place on an open network—

an environment in which an unauthorized user can pose as either a client or a server and intercept or tamper with communication between authorized clients and servers. Kerberos V5 authentication also provides secure and efficient authentication for complex networks of clients and resources.

The Kerberos V5 protocol uses secret key encryption to protect logon credentials that travel across the network. The same key can then be used to decrypt these credentials on the receiving end. This decryption and the subsequent steps are performed by the Kerberos Key Distribution Center (KDC), which runs on every domain controller as part of Active Directory.

Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography.

**The Internet is an insecure place.** Many of the protocols used in the Internet do not provide any security. Tools to "sniff" passwords off of the network are in common use by malicious hackers. Thus, applications which send an unencrypted password over the network are extremely vulnerable. Worse yet, other client/server applications rely on the client program to be "honest" about the identity of the user who is using it. Other applications rely on the client to restrict its activities to those which it is allowed to do, with no other enforcement by the server.

Some sites attempt to use firewalls to solve their network security problems. Unfortunately, firewalls assume that "the bad guys" are on the outside, which is often a very bad assumption. Most of the really damaging incidents of computer crime are carried out by insiders. Firewalls also have a significant disadvantage in that they restrict how your users can use the Internet. (After all, firewalls are simply a less extreme example of the dictum that there is nothing more secure than a computer which is not connected to the network --- and powered off!) In many places, these restrictions are simply unrealistic and unacceptable.

# Kerberos

1. Network access is requested

2. The KDC provides a (TGT)

**Authentication Service (AS)**

3. Access to a resource is requested (TGT)

**Kerberos client**

4. KDC issues an (ST) based on user rights

**Ticket Granting Service (TGS)**

5. (ST) is presented to the resource

**W2K DC/KDC**

**Print Server**

3-1
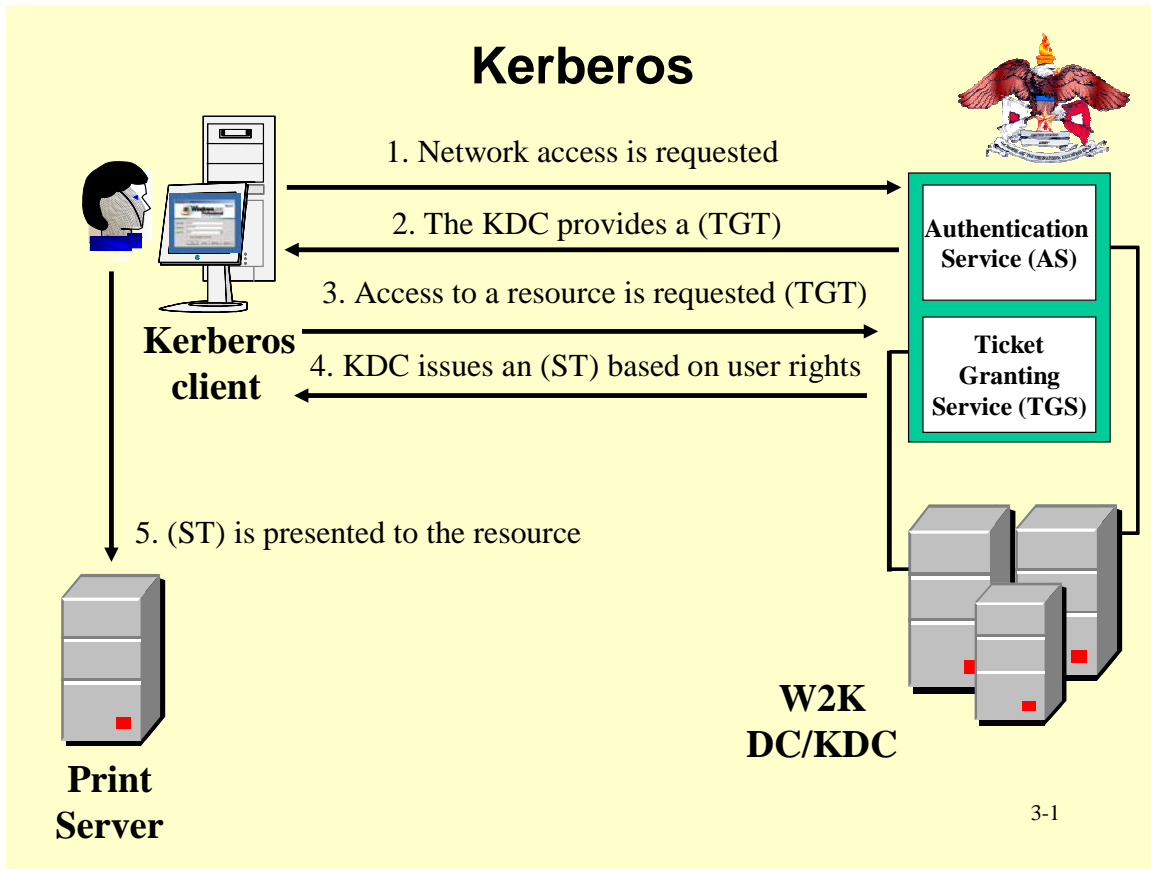
## Section 10 Security Tools

## Security Threat Avoidance Technology (STAT)

A software product that performs a complete security vulnerability and analysis of your Windows NT 4.0, Windows 2000/2003, and UNIX networks

Uses a unique database of over 3,000 Windows NT/Windows 2000/2003, Cisco Routers, HP Printers, Linux, Red Hat and UNIX® vulnerabilities (similar to a virus scanner in operation)

Vulnerabilities detected can be fixed using the AutoFixTM feature

## Minimum Software Requirements
- Windows 2000/NT 4.0 with SP 3 (or higher)

- Microsoft TCP/IP, NetBEUI, or IPX/SPX protocols

- Microsoft Data Access Component 2.5 or later

- Internet Explorer 4 (or higher)

- SSH protocol 1.5, 1.99, or 2.0 is required on UNIX systems

## Minimum Hardware Requirements
- PC or compatible:
    - Pentium 133 MHz (or higher) processor
    - 64 MB of RAM (128 recommended)
    - 800 x 600 monitor resolution
    - Hard drive with 40 MB of free space
    - CD-ROM drive or Internet connection

## Administrative Requirements

- For a full local vulnerability analysis, the user must be logged on with an account that has local administrator privileges
- To perform an analysis of other machines on the network, the user must be logged on with an account that has domain administrator privileges
- To analyze Windows 2000/NT workgroups, the user must have administrator privileges on every machine to be scanned.
- You need CSLA authorization to use this tool.

- POC is Julia Conyers-Lucero @ FT Huachuca
  DSN 879-8259, COMM (520) 538-8259
  E-Mail julia.conyers.lucero@csla.army.mil

- Need to pass training/testing 1st. Test site is online at
  Https://iatraining.us.army.mil

- Once authorized, you must update STAT's vulnerabilities database often.
  (usually every 1-2 wks)

**Orienting yourself with STAT**
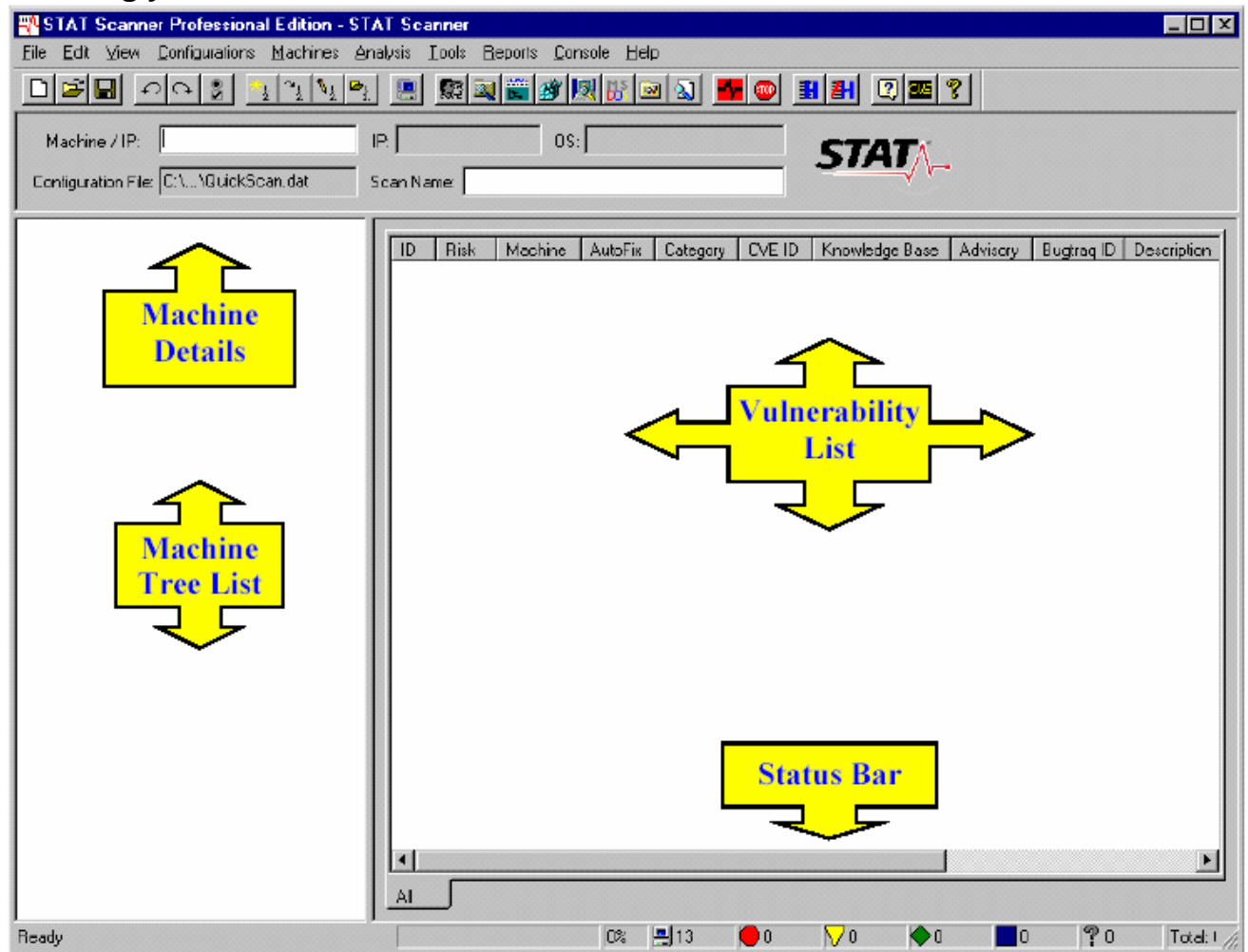
**Header**



The **Name** field displays the name of the computer or domain that is selected in the **Machine List**. The **IP** field displays the IP address of the computer that is selected in the **Machine List**. The **Configuration File** area of the **STAT Scanner Main screen** displays the current configuration (*.dat) file being used by the program.  The default configuration file is **vcid.dat**. The **OS** (Operating System) field displays the operating system of the computer that is selected in the **Machine List**.

**Vulnerability List**



**Machine Menu**

## Machine Selection Wizard
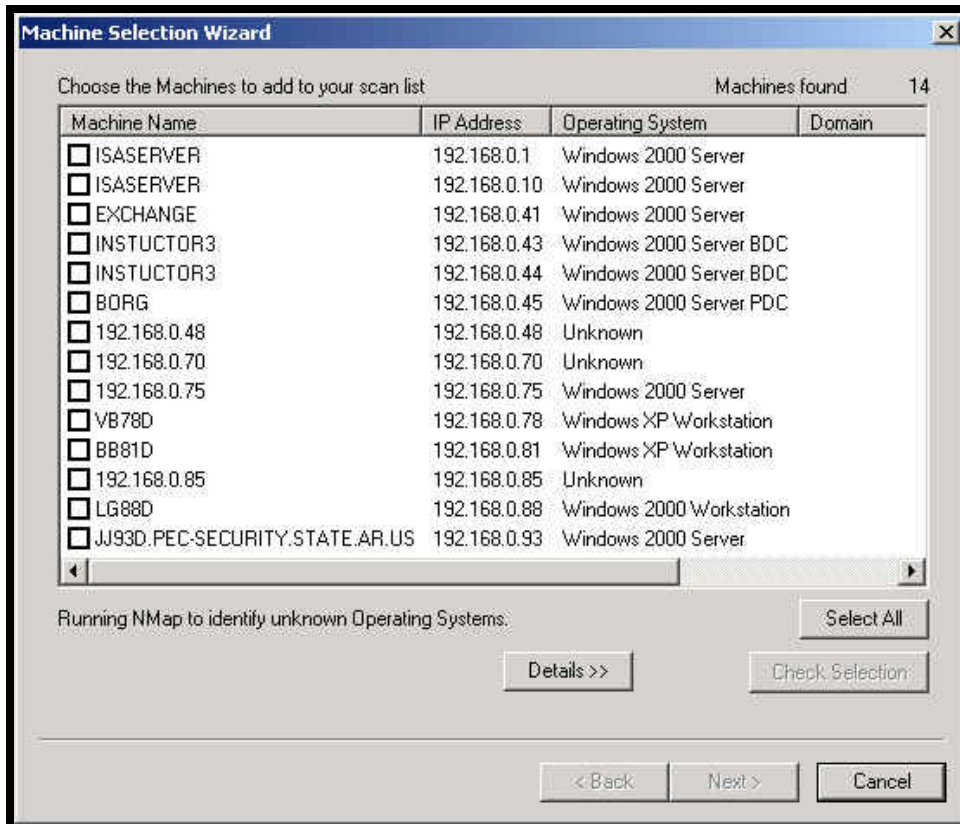
## Machine List
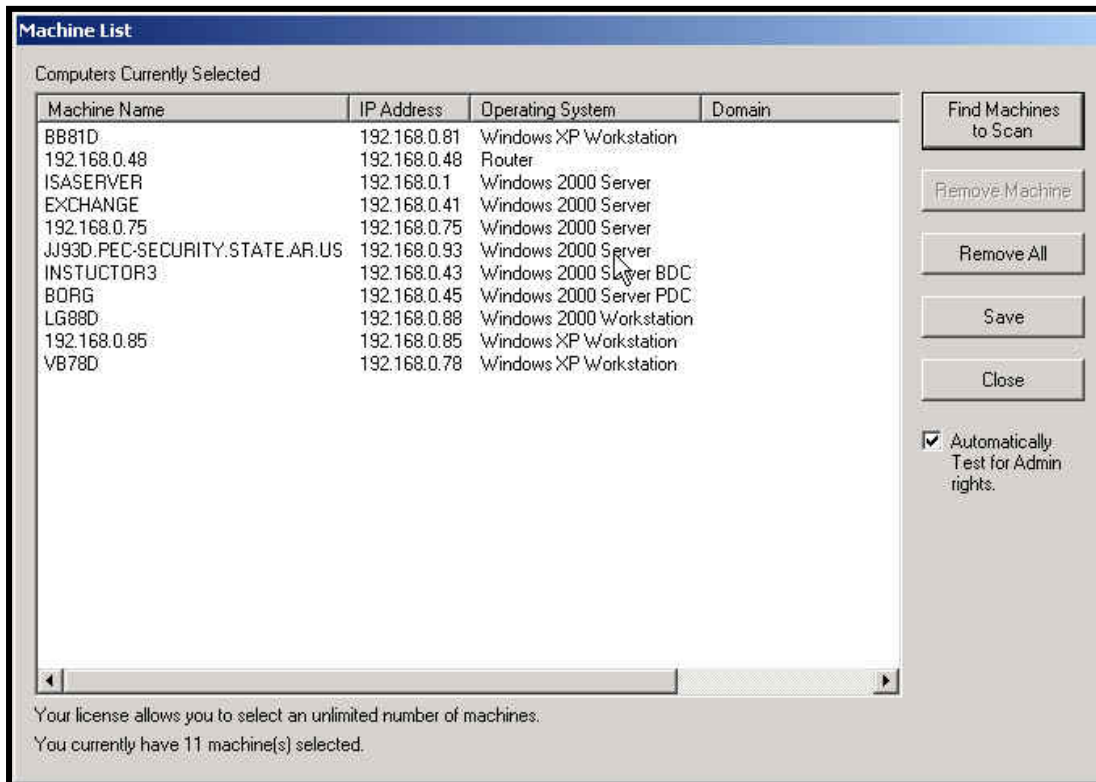
**Configuration**
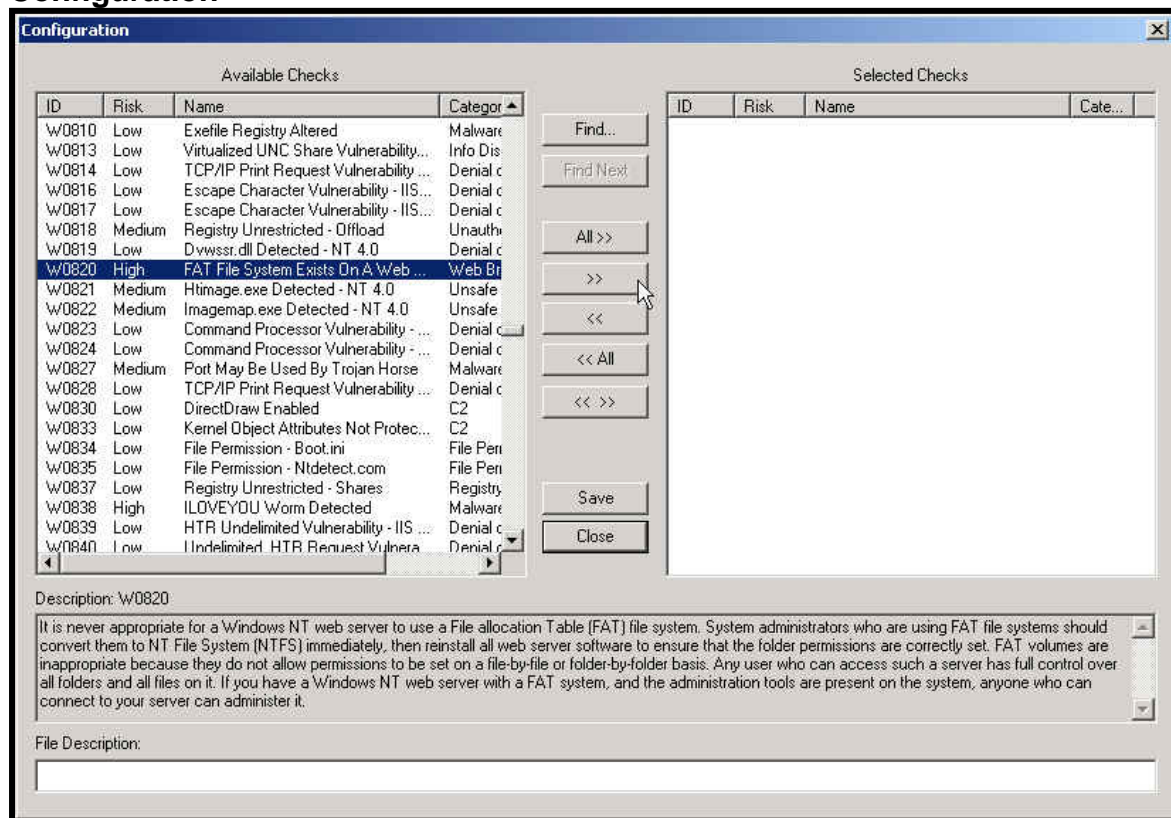


**Load Configuration From File**

Under the **Configurations menu**, select **Load Configuration From File**.  The Open display appears.
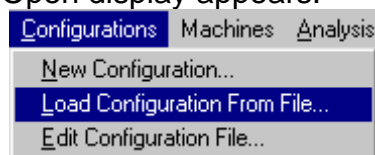


Select the Configuration (*.dat) file to be used.
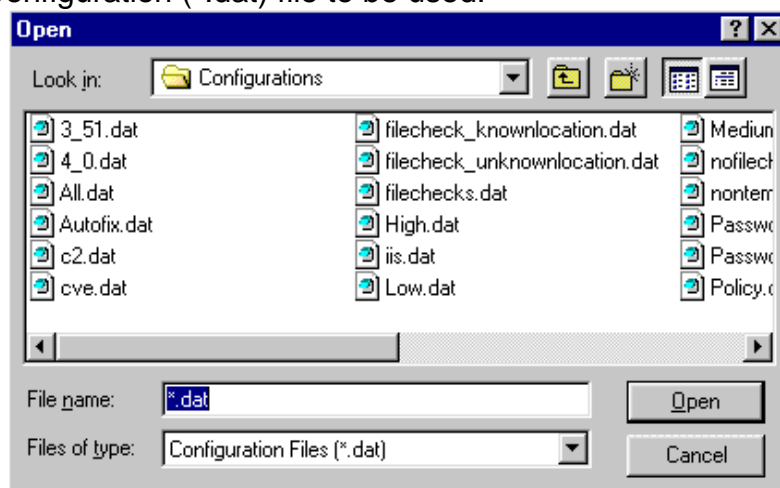


Click **Open**.

The file that is loaded is now the Current Configuration.  **STAT Scanner** will assess the selected machines for only the vulnerabilities contained within the selected file.

**Risk Levels**
**Vulnerabilities** are classified in five different levels of risks:

**High -** Grants unauthorized administrative access or privilege elevation to System or Administrator level**.**

**Medium -** Grants unauthorized access or serious denial of service.
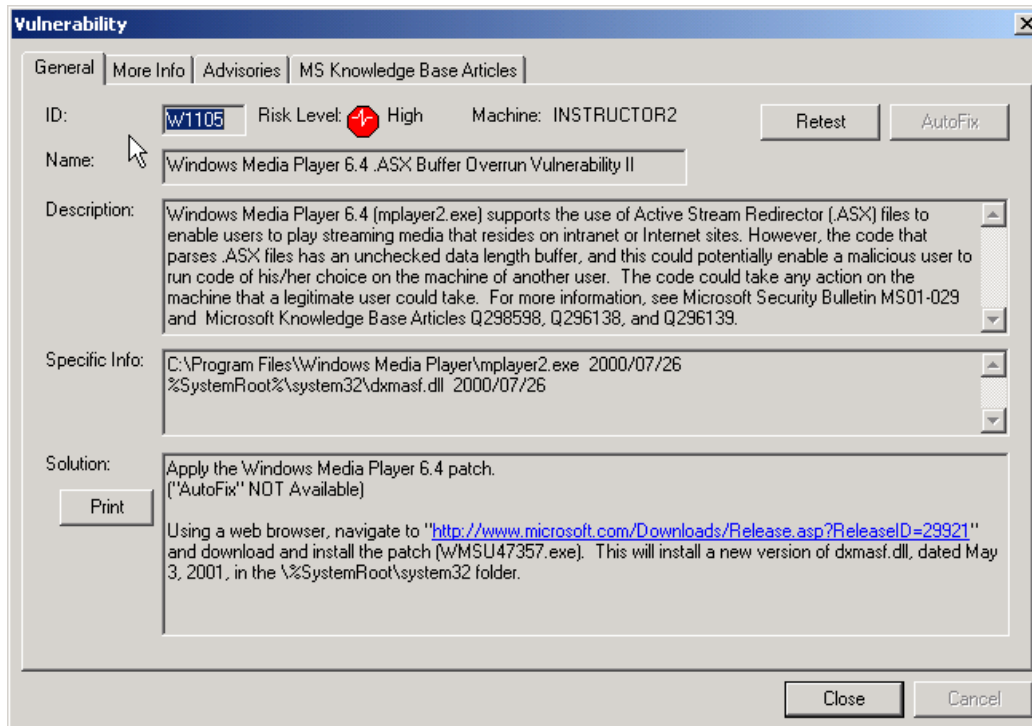
**Low -** Potential to grant unauthorized access or denial of service.

**Warning -** Recommended for good security practices.

**Unable To Assess** - STAT Scanner cannot assess the vulnerability.

**General Tab**
The **General Tab** provides a detailed description of a particular **vulnerability**, including any specific information (such as registry key or policy setting) and detailed **solution**.

## More Info Tab

The **More Info Tab** provides additional information on a particular **vulnerability**, such as type of **vulnerability**, **application**, and **web links** if available.
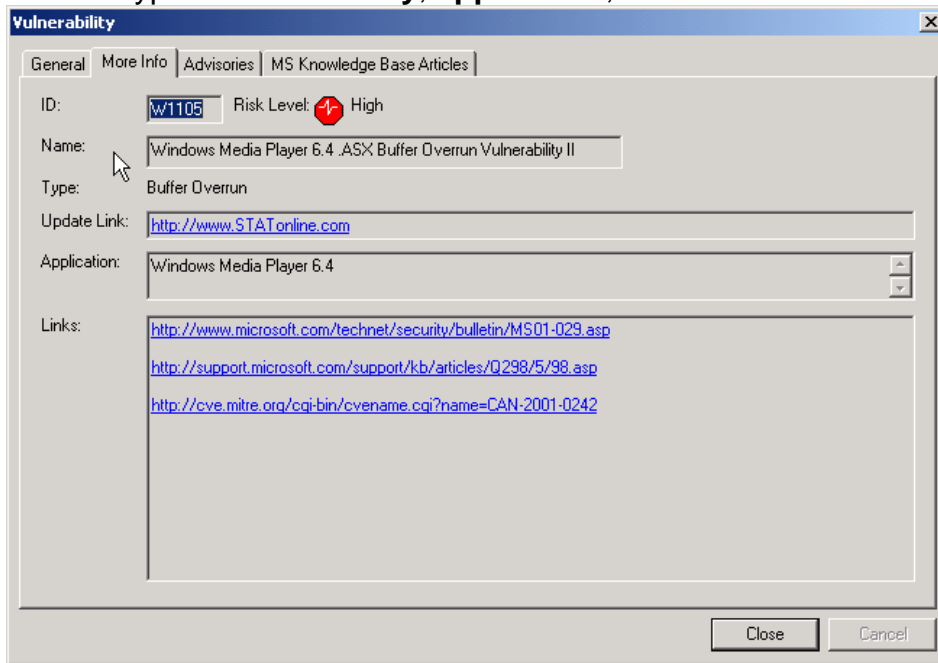


## Advisories Tab

The **Advisories Tab** provides a **security advisory**, if available, for a particular **vulnerability**. Advisories include **Microsoft Security Bulletins**, **CERT** Advisories, **CIAC** Bulletins, as well as other security advisories.
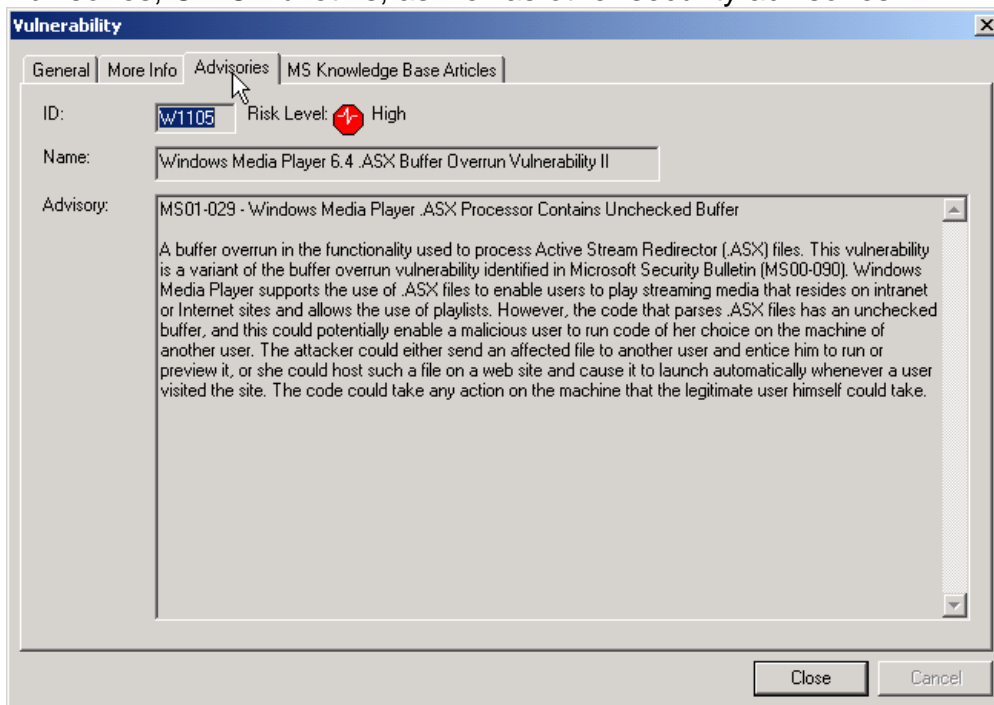
## Knowledge Base Tab
**The Knowledge Base Tab provides the Microsoft Knowledge Base article's,
if any, associated with a particular vulnerability** such as type of **vulnerability**,
**application**, and **web links** if available
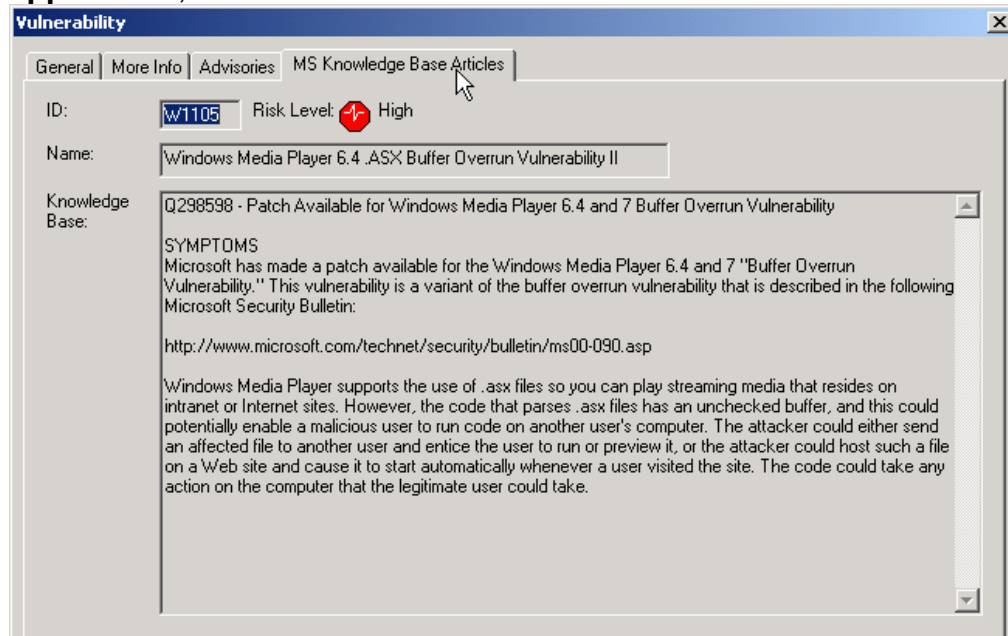


**Additional Information:**
The Department of the Army CIO/G-6 IAVA training site is in development. The
first training modules available from this site are Harris Stat Training Modules.
There are 3 modules for the Harris Stat training. You must register a User ID and
Password for this site before being allowed access to the training modules.
(http://iatraining.us.army.mil)
STAT Scanner has published a STAT-IAVA cross-reference file. This file does
not need to be requested and is available to any Army user with a licensed copy
of STAT Scanner. The file may be downloaded from RCERT CONUS or from the
STAT Premier Web Site, which is the same location for downloading program
updates.

**To download the IAVA mapping file from the Premier Web Site:**
1. Go to RCERT CONUS at www.rcert-c.army.mil/stat_index.html (you must
be at a .mil site) or https://premier.harris.com/stat/
2. Login (depends on download site)
3. Locate and Select "STAT Scanner - Army IAVA Configuration File" This is
the configuration file with the list of vulnerabilities the STAT program will use.
4. Locate and Select "army_iava_stat_scanner_vuln_mapping_1-27-03.pdf"
(The name of the file will change slightly each time it is released to reflect the
date of most current release).
5. Complete.

**eEye Retina Network Security Scanner**

eEye Retina Network Security Scanner is an automated IAVM tool that will provide network administrators and security personnel a mechanism for verifying application or non-application of Department of Defense (DoD) Computer Emergency Response Team (CERT) Information Assurance Vulnerability Management Notices. The IAVM tool will scan networks in order to mitigate security vulnerabilities found in software and those related to incorrect system configurations, as well as security issues related to policy and compliance. This proactive approach to security – eliminating vulnerabilities rather than thwarting attacks -- allows the DoD to better secure the vital digital assets under its control. The eEye Retina scanner is a network security scanner that allows the creation of custom scanning policies. These policies define which ports are scanned and which security audits are performed during a security assessment. The report generated by the Retina scanner includes audit results, open port analysis, detected services, share enumeration, and user account enumeration.

To install the eEye Retina Security Scanner, your server must meet at least the following minimum system requirements:
• Windows NT™ Version 4.0 SP3 or higher, Windows 2000 or 2003 Server
• Internet Explorer™ Version 4.01 or higher
• 32 MB of memory
• 16 MB of free disk space
• Internet connection (optional for remote scanning, required for regular updates)

 DISA recommends the following system:
• Windows 2000™ or 2003 Server
• Internet Explorer™ Version 5.5 or higher
• 512 mb of memory
• 1 gb of free disk space
• Internet connection

**Administrative Requirements**

•   You need CSLA authorization to use this tool.
•   POC is Julia Conyers-Lucero @ FT Huachuca
•   DSN 879-8259, COMM (520) 538-8259
•   E-Mail julia.conyers.lucero@csla.army.mil
•    Need to pass training/testing 1st. Test site is online at
        https://iatraining.us.army.mil
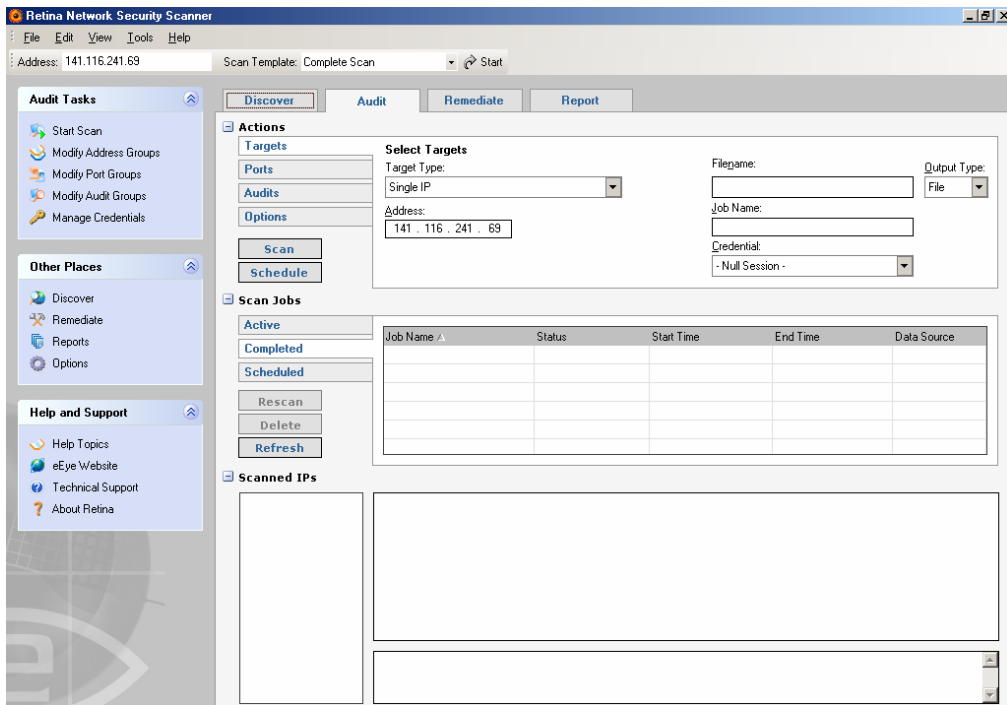
**Above is the Main Screen of Retina.**

## LAN Manager Authentication Requirements

**B.1.2** click on LAN Manager Authentication Level
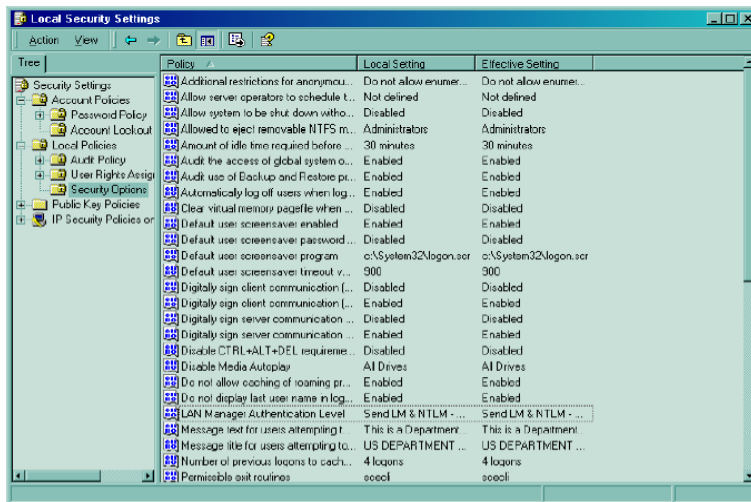


Click Start, click Programs, click Administrative Tools, double click Local Security Policy, expand Local Policies by clicking the plus sign, click on Security Options . LAN Manager must be set at "3"
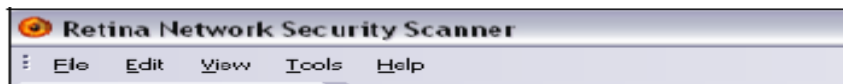
**B.1.4** Right click LAN Manager Authentication Level and click on Security. Local policy setting must be set to second item on drop down menu. This is setting *"Send LM & NTLM – use NTLM2 session security if negotiated",* click OK.



NOTE: If it is set to any other settings Retina will not be able to access the registry of the host system remotely.

## Starting Retina Menu Bar



The following drop-down menus are provided from the Retina Interface:

File – to open scan files and set DSN locations

Edit – normal cut, copy and paste editing functions

View – display or hide the Quick Scan, Explorer or Status bars.

Tools – audits and plug-in wizards; access to address, audit and port group modification dialogs; credential management; updates and program options

Help – links to product help, support, eEye sales, license management and information about the product version

## Retina Shortcut Bar



**Retina has four main tabs. They are Discover, Audit, Remediate Tab and the Report Tab.**
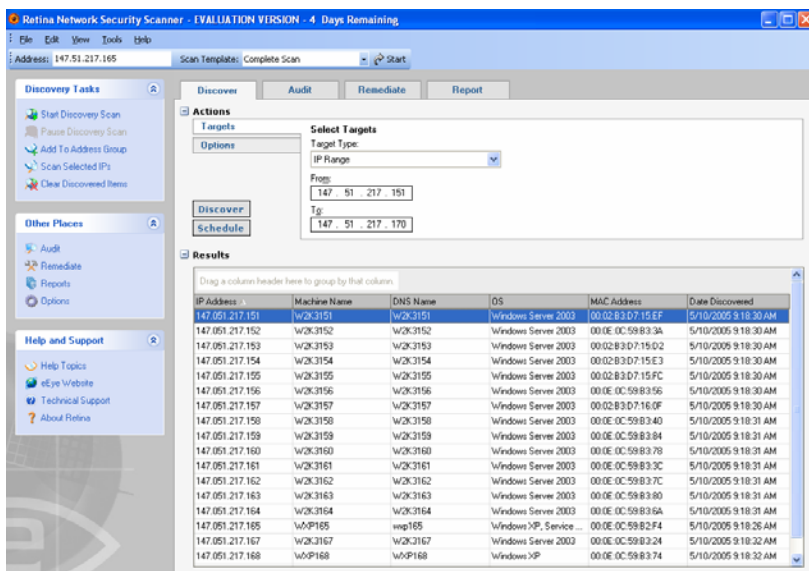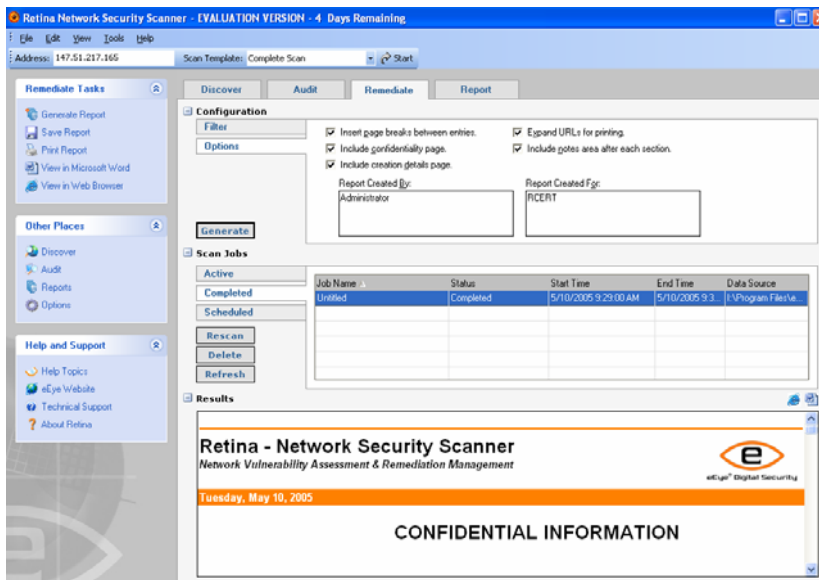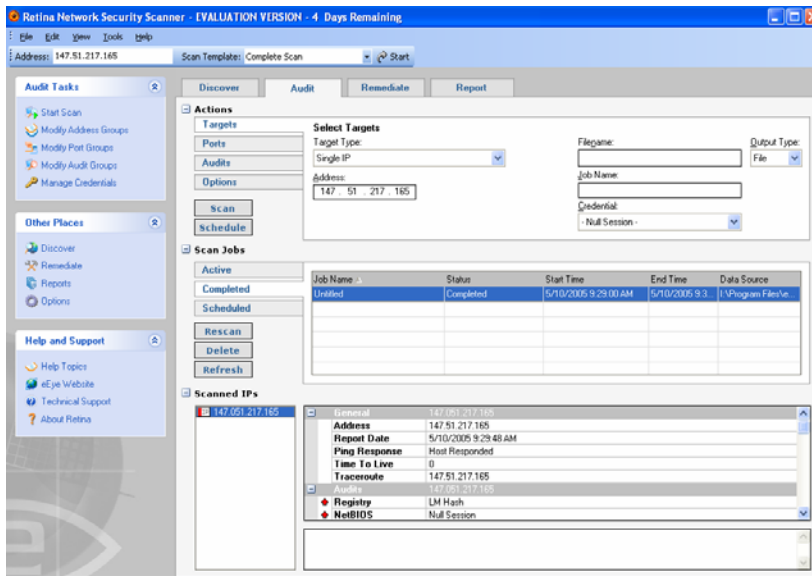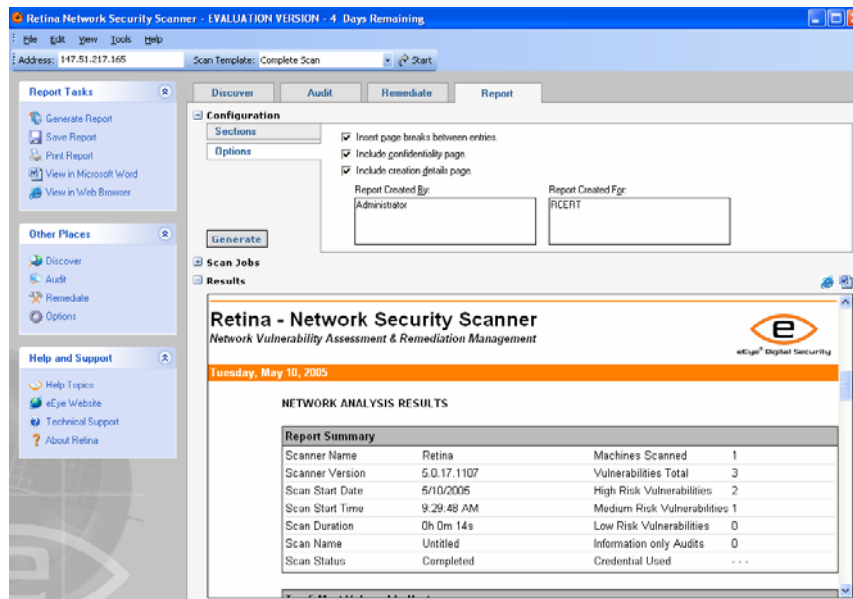
**Risk Levels**

- Information
    - A security vulnerability that gives the attacker more information, which helps them to target their attacks more successfully.
- Low
    - Low-risk vulnerability usually include vulnerabilities that can be exploited to read files containing public information, or a vulnerability that gives an attacker very minimal access to a remote system.
- Medium
    - Medium Level usually includes vulnerabilities that can be exploited to gain general access to a system.
- High
    - Full remote access. A vulnerability that can be exploited to gain total access of a machine remotely falls under this category. Extremely severe and tools to exploit them are usually publicly available.

**Retina Extras**

- Command Line execution
- Auto Update/Manual Update
- Scans are automatically saved.
- Accuracy – able to scan a class C network in 20 min.

**ISS Internet Scanner**

The ISS Internet Scanner allows you to scan remote computers for security policy compliance. Within the IIS Internet Scanner, you can reflect your company's security policies by defining custom scan policies. These scan policies define the baseline security requirements for your company and indicate which vulnerability checks are included in a scan session. Once you define a scan policy, you can implement the scan against one or more hosts on the network, depending on your ISS Internet Scanner license issued by your supporting RCERT.  ISS Internet Scanner is used in the DITYVAP classes offered by your RCERT.  The course is required prior to running ISS Internet Scanner.

**MBSA**
**MICRSOFT BASELINE SECURITY ANALIZER**

The MBSA tool allows you to assess the security configuration of one or more Windows-based computers. MBSA performs two major tasks:

- Scans for missing service packs and security updates. MBSA determines which hotfixes and service packs are not applied to a target computer. The MBSA tool can also filter the list of missing updates and service packs based on approved updates configured at a Microsoft Software Update Services (SUS) server.
- Scans the Windows OS, Microsoft Internet Information Services (IIS), Microsoft SQL Server, desktop applications, Windows Media Player, and Microsoft Exchange Server for common security misconfigurations.

The MBSA tool can be executed from both a GUI and from the command line. Both versions of MBSA perform the tests above.

**Requirements for Running MBSA**

The requirements for running MBSA vary, depending on the type of scan you are performing and whether you are scanning the local computer or performing a scan against remote computers. To perform a security assessment of the local computer, the following requirements must be met:

- The user must be a local Administrator of the target computer.
- The computer must be running Windows 2000, Windows XP or Window 2003.
- The computer must have Internet Explorer 5.01 or later.

MBSA can be found on the Microsoft Security Website:
http://www.microsoft.com/technet/security

**SECURITY CONFIGURATION MANAGER TOOLSET**

Windows Server includes a group of related tools—Security Templates, Security Configuration and Analysis, and so forth—that provide security-specific functionality. Windows Server primary security tools include:

- Security Templates, and Security Configuration and Analysis—These two MMC snap-ins, which are discussed in the next section, make applying consistent security settings across your organization easier.
- Security Settings extension to Group Policy—This tool makes editing the security information on a domain, a site, or an organizational unit (OU) within Active Directory easy.
- Local Security Policy—This MMC snap-in edits the security configuration of a local computer, including its password policy and other security settings. A similar snap-in on domain controllers enables you to edit these security properties for an entire domain.
- Secedit.exe—This command-line tool applies or analyzes security templates. Its nongraphical interface makes it ideal for use in batch files.

Windows Server includes another tool we especially like, called Hfnetchk.exe (which stands for HotFix NETwork CHecKer). Hfnetchk.exe is designed to analyze Windows computers and let you know whether they're missing any recent security updates.

**Security Templates Snap-in**

The Security Templates snap-in is the best place to start. The snap-in starts with a list of the templates that are included with Windows Server 2000/2003:

Compatws—Designed to lower specific file system and Registry permissions to enable some older Windows applications to run properly.

DC security—Designed to be applied to domain controllers, it provides a higher level of security.

Hisecdc—An even more secure configuration for domain controllers, it requires network encryption from clients.

Hisecws—A highly secure configuration that enables IPSec encryption with secure servers. This template can be applied to workstations and member servers in a domain.

Securedc—A slightly less-secure template than Hisecdc, intended for use on domain controllers.

Securews—A slightly less-secure template than Hisecws, intended for use on workstations and member servers.

145

**Security Templates**

There are four categories of pre-built security templates:

Basic

Secure

High Secure

Miscellaneous

The basic, secure, and high security templates represent increasing levels of security. The miscellaneous templates include compatibility templates, optional components templates, and original setup security templates.

The basic templates include:

Basicdc: Applies a basic level of security for domain controllers.

Basicsv: Provides a basic level of security for file and print servers.

Basicwk: Provides a basic level of security for workstations


Higher-level security templates include:

Securedc: Provides a higher level of security for domain controllers

Securews: Provides a higher level of security for workstations

The following templates provide the highest level of security for Windows -based computers but are not compatible with network connectivity with other downlevel Windows operating systems:

Hisecdc

Hisecws

There are plenty of built-in security templates that you can choose from. These templates are categorized for domain controllers, servers, and workstations. These security templates have default settings which have been designed by Microsoft. You can find all of these security templates in the root drive\Windows\Security\Templates folder for Windows 2003 and root drive\Winnt\Security\Templates for 2000. Here is a list of the security templates that you will find in this folder.

Compatws.inf – This is required by older applications that need to have weaker security to access the Registry and the file system.

DC security.inf – This is used to configure security of the Registry and File system of a computer that was upgraded from Windows NT to Windows 2000/2003.

Hisecdc.inf – This is used to increase the security and communications with the domain controllers.

Hisecws.inf – This is used to increase security and communications for the client computers and member servers.

Notssid.inf – This is used to weaken security to allow older applications to run on Windows Terminal Services.

Ocfiless.inf – This is for optional components that are installed after the main operating system is installed. This will support services such as Terminal Services and Certificate Services.

Securedc.inf – This is used to increase the security and communications with the domain controllers, but not to the level of the High Security DC security template.

Securews.inf – This is used to increase security and communications for the client computers and member servers.

Setup security.inf – This is used to reapply the default security settings of a freshly installed computer.

Security Templates essentially are text files. Anyone gaining access to root could create his or her own templates that would affect system security on a forest wide basis depending on the affected servers' placement. The use of secedit.exe tool should be restricted to only administrators.

To Implement Security Templates

From MMC console, select the Security Templates snap-in

- Double-click the Security Templates icon to open it.
- Double-click the folder icon to open it and see the included templates
- Double-click the appropriate policy template to open it.
- Make appropriate policy selections
- In the left pane of the MMC window, right-click on the appropriate policy template icon. Select Save as. Save the policy with an appropriate name.
- Open the Event Log Settings for appropriate name to make sure you changes were saved.

- Close the Security Templates namespace.
- Right-Click the Security configuration and Analysis icon and select Open Database
- Enter a filename of appropriate name and click Open
- When prompted for a template to import, select the appropriate name and click Open
- Right-click the Security configuration and Analysis icon and select configure Computer Now.

When adding additional templates to an open security database, the effect is cumulative.

## Security Configuration and Analysis MMC Snap-in

The Security Configuration and Analysis MMC snap-in performs security analysis by comparing the current state of system security against an analysis database. During the creation, the analysis database uses at least one security template. If you choose to import more than one security template, the database will merge the various templates and create one composite template. The database will resolve conflicts in order of import—the last template that is imported takes precedence.

To analyze the current security settings of a local computer by using the Security Configuration and Analysis MMC snap-in, follow these steps:

1. Open a blank MMC and add the Security Configuration and Analysis MMC snap-in to it.
2. In the console tree, right-click Security Configuration and Analysis and click Open Database.
3. In Open Database, create a new database by entering a name for the database in the File Name field and click Open.
4. In the Import Template window, select the Setup Security template and click Open.
5. In the details pane, right-click Security Configuration and Analysis and then click Analyze Computer Now.
6. In the Error Log file path, click OK to create a log file in the default location.

Say you want to analyze a Windows computer to compare its security settings to the default policy that gets applied during installation.

You can use the output of the analysis to perform a side-by-side comparison of the security settings. The Security Configuration and Analysis MMC snap-in displays the result of the analysis by using the icons described in the chart below.

Output of the Security Configuration and Analysis MMC Snap-In

| Icon | Description |
|---|---|
| Red X | The entry is defined in the analysis database and on the system, but the security setting values do not match. |
| Green check | The entry is defined in the analysis database and on the system, and the setting values match. |
| Question mark | The entry is not defined in the analysis database and therefore was not analyzed. This occurs when a setting was not defined in the analysis database or when the user running the analysis did not have sufficient permissions. |
| Exclamation point | This item is defined in the analysis database but does not exist on the actual system. |
| No highlight | The item is not defined in the analysis database or on the system. |

## SECEDIT.EXE COMAND-LINE UTILITY

The Secedit.exe command includes all the functionality of the Security Configuration and Analysis MMC snap-in and has the ability to force a refresh of Group Policy in Windows 2000. In Windows XP/2003, you may use the Gpupdate.exe command-line utility to force a refresh of Group Policy. By calling the Secedit.exe command-line tool from a batch file or automatic task scheduler, you can use it to automatically apply templates and analyze system security.

## SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG)

The STIGs were initially developed to assist the sites in securing their systems against security and infrastructure vulnerabilities.  All sites have a vested interest in maintaining system security, as it directly impacts the site's Certification and Accreditation (C&A).  Sites are mandated by DISA to have a valid C&A status by the authority derived from DOD Directive 5200.28, Security Requirements for Automated Information Systems, 21 March 1988, and the Computer Security Act of 1987, Public Law 100-235, January 1988.  The requirements for accreditation of DISA Information Technology, as described here, are found in DISAI 630-230-19, DISA Information Systems Security Program, July 1996.

This process has been extended to Joint Commands seeking to secure their systems against the same vulnerabilities.  While there is no mandate for their use at the Joint Commands, the value of the STIGs has been seen by each of the Unified Commands.  Compliance with the applicable Security Technical Implementation Guide (STIG) is mandatory for systems residing in a DISA facility and for any system directly administered by DISA.  The use of the principles and guidelines in this STIG will provide an environment that meets or exceeds the security requirements of DOD systems operating at the C2 system high level or EAL3 level, containing unclassified but sensitive information.  In the interest of

promoting enhanced security for systems both inside DOD and within the Federal Government's computing environments, DISA encourages any interested DOD activity or party to obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site.  This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information.

The NIPRNet URL for the IASE site is http://iase.disa.mil/.  The DISA Field Security Operations URL is http://guides.ritchie.disa.mil/.  Access to the STIGs on the IASE web server requires a network connection that originates from a **.mil** or **.gov**.  The STIGs are available to users that do not originate from a **.mil** or **.gov** by contacting the FSO Support Desk at DSN 570-9264, commercial 717-267-9264, or e-mail to **fso_spt@ritchie.disa.mil**.

## DISA GOLD DISK

DISA has a library of STIGs for Windows and Unix OS, Web servers, databases and network devices.  But guidelines alone cannot configure systems, so DISA came up with the Gold Disk to apply settings and vendor patches, validate and maintain compliance, and report system status.

DISA Gold Disk Main Window Pre-Scan

The Gold Disk Main Window shown below appears after the program has been fully loaded and initialized.  Some of the key elements of the Main Window are listed below:

- Title Bar – contains the current Gold Disk version number, in this case, Build 1.0.0.482.

- Menu Bar – displays the drop down menu options (File, View, Tools, Window, Help)

- Tool Bar – displays current valid actions (Setup Scan, Exit Program).  The valid options will change based on the state of the program.

- Message Display Area – displays the following information:
    o Total Number of Vulnerabilities loaded
    o Number of Category 1 Vulnerabilities
    o Number of Category 2 Vulnerabilities
    o Number of Category 3 Vulnerabilities
    o Number of Category 4 Vulnerabilities
    o Number of Uncategorized Vulnerabilities

- Scan Button – Initiates scan of system when selected

- Scan Progress Bar – graphically displays scan progress

- Policy Drop Down Box – allows user to choose a scan/fix policy.  Two policies are currently supported, DISA Gold and DISA Platinum.  The default policy is DISA Platinum.

  DISA Gold is designed to configure the respective Windows operating system or application(s) to meet the FSO Gold Standard.  This is the minimum level of security required for connecting a new machine to the network.  Operational impact was considered when this collection of configuration settings was established; therefore, we are providing a high level of assurance that the functioning of the box or installed applications will not be impaired.  The Gold Standard is not used for certifying or accrediting a site, but is the base level upon which to begin configuring additional requirements for security.


  DISA Platinum is designed to configure an operating system or application and bring the system into compliance with the applicable STIG.

- Status Bar – updates in real-time to display check/fix module that is currently being performed.  The initial state of the status bar is "Ready…"
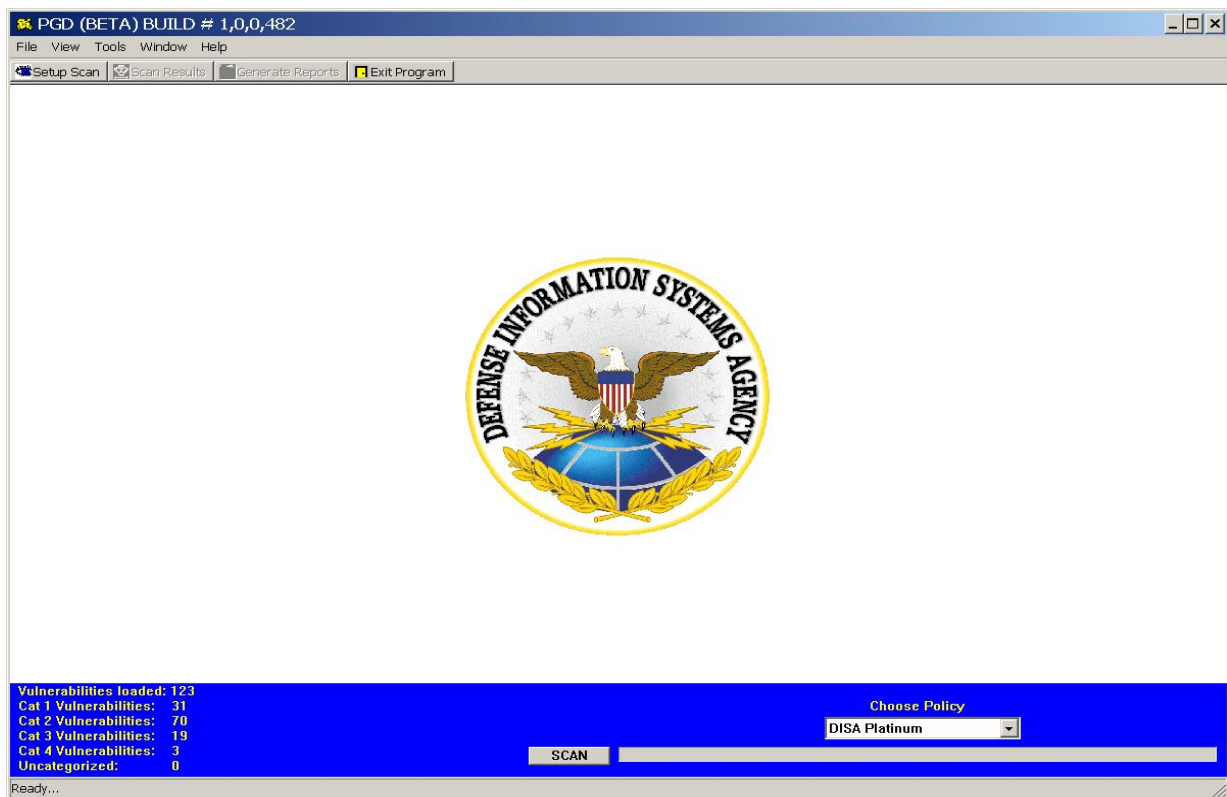
The check status can be one of the following states:

| Symbol | Description |
| --- | --- |
| | OK – Not a finding (Green Circle "OK" icon) |
| | I – Category 1 finding (Red Circle "I" icon) |
| | II – Category 2 finding (Yellow Circle "II" icon) |
| | III – Category 3 finding (Dark Blue Circle "III" icon) |
| | IV – Category 4 finding (Light Blue Circle "IV" icon) |
| | Manual – Manual Check (Grey Circle "Red - ?" icon) |
| | Error – Check Error (Grey Circle "Red - ! icon) |
| | Fix successful during the fix session in the fix window. |
| | Fix failed during the fix session in the fix window. |
| | Validation successful during the fix session in the fix window. |
| | Validation failed during the fix session in the fix window. |

The checks are logically grouped within the tree view based on the type of check being performed.  The high-level check categories for are:

- Account Policy Checks

- Audit Policy Checks

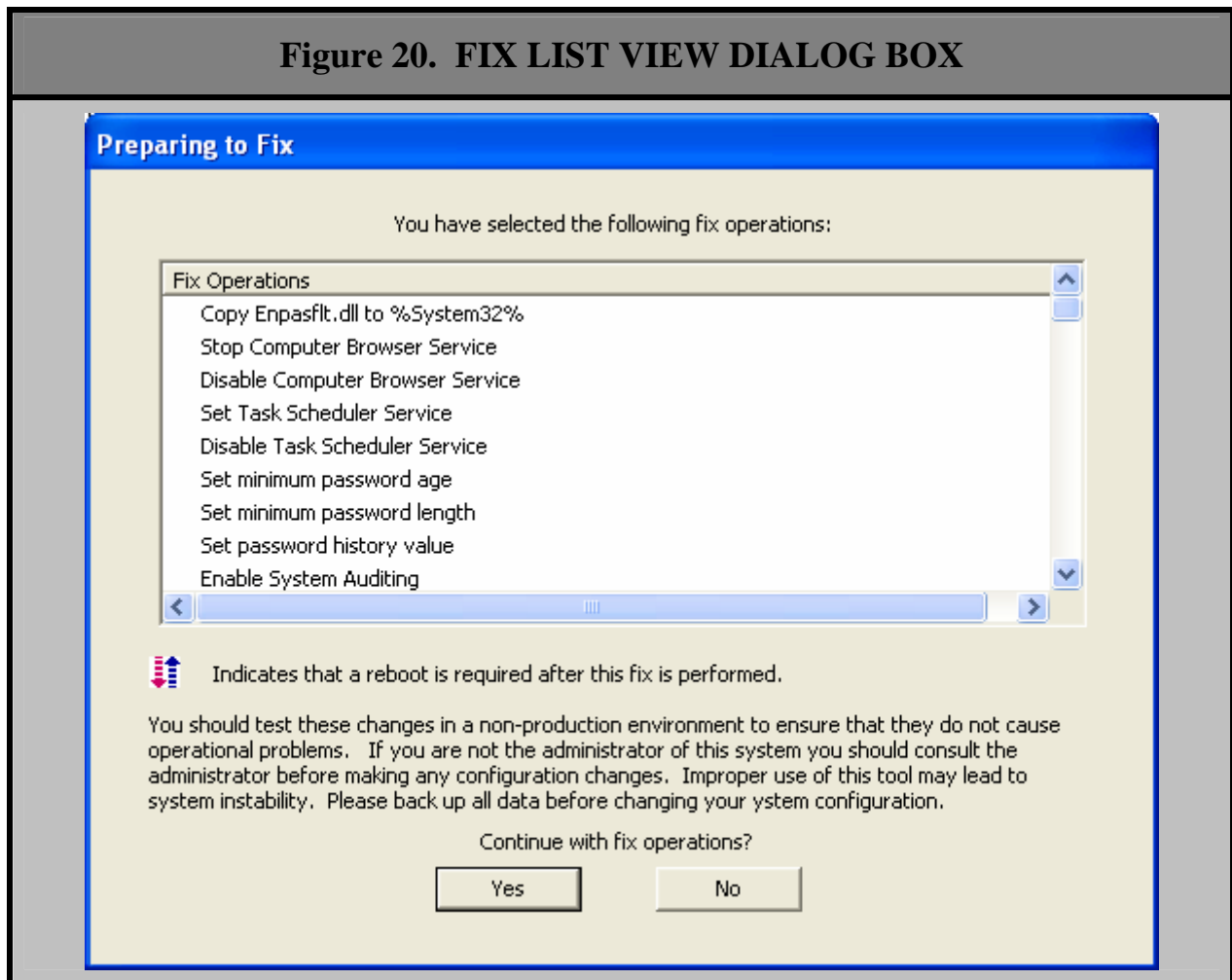- File System Checks

- Registry Checks

- Security Options

- Service Packs/Hotfixes/IAVM

- Manual

- Services

- User Rights

**Figure 9.  GOLD DISK MAIN WINDOW SCAN RESULTS DETAIL**
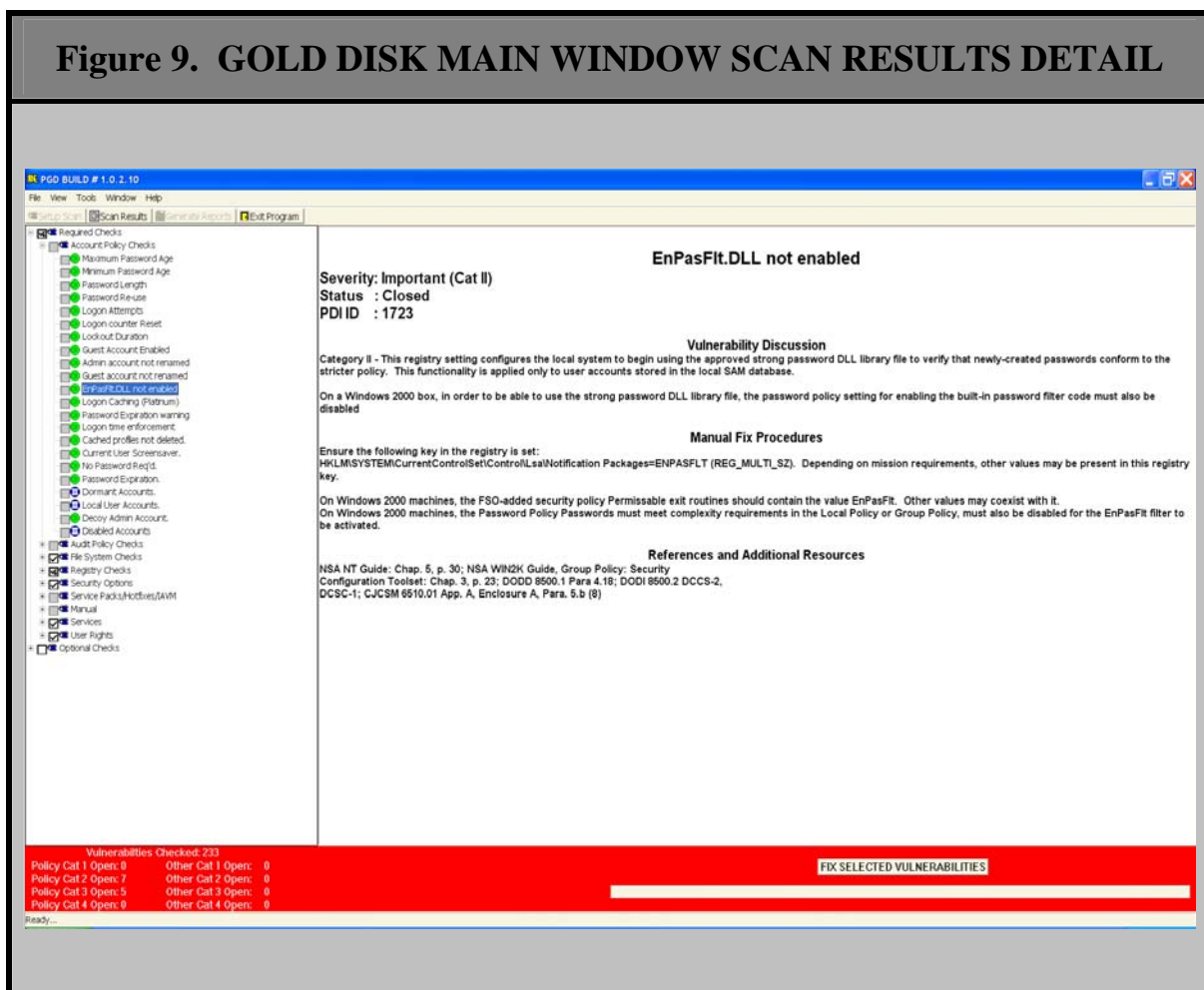
This list view is provided as a final informative step before automated corrections are conducted. The window provides a scroll feature on the right side and bottom of the window as depicted below:

## Figure 20.  FIX LIST VIEW DIALOG BOX

**Preparing to Fix**

You have selected the following fix operations:

Fix Operations
- Copy Enpasflt.dll to %System32%
- Stop Computer Browser Service
- Disable Computer Browser Service
- Set Task Scheduler Service
- Disable Task Scheduler Service
- Set minimum password age
- Set minimum password length
- Set password history value
- Enable System Auditing

Indicates that a reboot is required after this fix is performed.

You should test these changes in a non-production environment to ensure that they do not cause operational problems.   If you are not the administrator of this system you should consult the administrator before making any configuration changes.  Improper use of this tool may lead to system instability.  Please back up all data before changing your ystem configuration.

Continue with fix operations?

Yes          No

**Section 11 - Practical Exercises**

**NTFS ADS Practical Exercise**

**NOTE:  All command will be performed inside of the Streams directory from the Command Prompt.**

Please retain from the instructor the appropriate drive letter or partition to use*.* This PE will be performed on Windows 2003 drive.  To Open Command Prompt Click on **Start**->**Run**, then type **cmd**.

1.  Open Command Prompt and type in the following commands:
    >            **cd \streams**
    >            **echo This is a normal text file > normal.txt**
    >            **type normal.txt**
    >            **dir normal.txt**

    From the output, you should notice the text "***This is a normal text file***" appear from the type command.  You should also have a directory listing for the file normal.txt.

    What is the size of the file? _____


2.  Type the following command:

    **notepad normal.txt:hidden.txt**

    Click **Yes** to create file, and type the following text

    **This is a hidden text file**

    Click **File > Save**, then **File > Exit.**

3.  Type the following command:

    > **Dir**

    Was there a file hidden.txt?  **YES / NO**

    What is the file size of normal.txt? _____

    Did the file size change from step 1?  **YES / NO**
    (will not detect the presence of these newly created ADS)

4. Type the following command:

>   **more < normal.txt:hidden.txt**

    Did you see the text "**This is a hidden text file**"?   **YES  /  NO**

5. Type the following command:

>   **type \windows\notepad.exe > normal.txt:np.exe**
>   **type \windows\system32\calc.exe > normal.txt:c.exe**

6. Type the following command:

>   **notepad normal.txt:test.vbs**

    Click **Yes** to create file, and <u>type</u> the following text (<u>remember </u>to click your
    enter key after typing your script.)

**MsgBox "Hello World!!! This could be a malicious script"**

    Click **File > Save**, then **File > Exit.**

7. Type the following command:

>   **streams normal.txt**
>   **dir normal.txt**

    What ADS files are attached to the file normal.txt?

    _____

    _____

    _____

    Was there a change in the file size of normal.txt?  **YES / NO**

**In the next couple of steps we are going to execute a couple of ADS
programs in normal.txt**

8. Type the following command:

>   **Start .\normal.txt:c.exe**

    Are we able to execute the calculator program?  **YES / NO**

9.  Type the following command:

    **Start .\normal.txt:test.vbs**

    Did you get a message box with "Hello World!!! This could be a malicious script"?  **YES / NO**

    Currently there are no antivirus products capable of detecting NTFS ADS.

    Are NTFS ADS a security risk?  **YES / NO**

    Why?

    _____

    _____

    What sort risk rating would you give NTFS ADS?  **HIGH  /  MEDIUM  / LOW**

    Why?

    _____

    _____

    Should we replace NTFS with FAT/FAT32 to avoid NTFS ADS?  **YES  / NO**

    Why?

    _____

    _____

    Should we be scanning our system(s) for NTFS ADS usage?  **YES  /  NO**

    If so, how often? _____

REQUIREMENTS:
Windows NT/2000/XP/2003 with NTFS partition
streams.exe from SysInternals
(http://www.sysinternals.com/ntw2k/source/misc.shtml)
or  lads.exe from Frank Hayne Software
(http://www.heysoft.de/Frames/f_sw_la_en.htm)

**Permissions Practical Exercise**

This practical exercise will provide hands-on experimentation with file permissions including inheritance.

Please retain from the instructor the appropriate drive letter or partition to use in place of *Windows 2003 Server.*

1. Log on locally to the Windows 2003 Server, using the administrator account (pwd = student).

2. Select **Start**->**Programs**->**Accessories**->**Windows Explorer**

3. Open the root of the Windows 2003 Server (MyComputer\W2K3Server). Instructor will provide the drive letter.

4. Create a new folder name stage1.  On the right-hand side panel, **right-click** and select **New**->**Folder** or use the File Menu dropdown.

5. **Right-click** the folder, stage1.

6. Select **Properties**.  On the Properties Window select the **Security tab**.

7. On the Properties window, click on **Advanced**

8. Clear the **Allow inheritable permissions from parent to propagate to this object checkbox and all child objects**.

9. On the Security window, select Remove to discard all inherited ACEs.

10. On the Advanced Security window, select **Administrator**, click **Remove**, click **OK,** click **Yes**.

11. On Stage1 Properties, click **ADD**.  On the Select Users or Groups Window, click **Advanced**, Click **Find Now**.

12. Select the **Administrators group** and hold down the **Ctrl key** and select the **Everyone group**.  Click **OK** twice.

13. On the properties windows, configure two ACEs: **Administrators**: Full Control, **Everyone**: Read & Execute, List folder Contents and Read.

14. Click **OK** to save the new ACL.

15. Open the stage1 folder (**double-click** folder to open)

16. Create a subfolder inside folder stage1, named stage2.  On the right-hand side panel, **right-click** and select **New**->**Folde**r or use the File Menu dropdown.

17. Right click on the stage2 folder. Select Properties.  Select the **Security Tab**.  Verify the default ACL on the stage2 folder.  How is the ACL defined?

_____

_____

18. Click on **Advanced,** unselect "**allow inheritable permissions from parent to propagate to this object**".  Click on **copy** when the security box appears.  Click **OK** on the Advance Security Setting Window for Stage2.

19. Click **OK** to close Stage2 properties box.

20. Open the stage2 folder (**double-click** folder to open).

21. Create a new text file named **file1.txt**.  On the right-hand side panel, **right-click** and select **New**->**Text Document** or use the File Menu dropdown.

22. **Right-click** file1.txt.  Select **Properties**.  On the Properties Window, select the **Security tab** and verify the permissions.
How is the ACL defined?

_____

_____

23. Close the Permissions window for file1.txt by pressing the **OK** button.

24. Click on the **back button**, right click stage2, select **Properties**, and select the **Security Tab** to open the Permissions window for stage2.

25. Click **Add**, Click **Advanced**, then Click **Find Now**.

26. Select **labuserXa**, click **OK** twice, click box for **Deny Write**.  This will add an ACE to explicitly deny write access to user labuserXa.

27. Click **OK**.

28. Select **YES** to the Security Caution window.

29. Open stage2 (double-click) and **right-click** on file1.txt, select **Properties**, select the **Security Tab** and verify the permissions.
How is the ACL defined?

ㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡ

ㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡ

30. Close the Properties Box, by selecting the **OK** button.

31. Click on the **back-button**, **right-click** stage2, select **Properties**, select the **Security Tab** to open the Permissions window for stage2.

32. Click **Add**, Click **Advanced**, then Click **Find Now**.

33. Add an ACE to explicitly granting write access to authenticated users. Select **authenticated users group**, click **OK** twice, and click **Allow Write**.

34. Click **OK**.

35. Log off of the administrator account.

36. Log in as the labuserXa account (password = LUXX-p@$wd).

37. Select **Start**->**Programs**->**Accessories**->**Windows Explorer**

38. Drill down to the stage2 folder (double-click MyComputer\W2K3server drive\stage1\stage2).

39. Attempt to create a new text file named file2.txt.  **Right-click** and select **New**->**Folder** or use the File Menu dropdown.  Was the new file successfully created?

ㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡ

40. Open the **file1.txt** file.  Attempt to make changes to the file and save it. Was the file modification successful?

ㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡㅡ

41. Close all windows.

42. Log out.

43. Wait for instructor review.

**Encrypting File System Practical Exercise**

1. **Logon** as Administrator with proper password.

2. **Create** a folder on the root directory named **AdminEncrypt**.

3. **Encrypt** the folder. (**Right click** on the folder, choose **properties**. On the AdminEncrypt Properties Dialog Box, click on **advanced**. Check the box "**Encrypt contents to secure data**". Click on **ok** twice to close the dialog box. The folder's detailed information should now appear green.)

4. **Create** a text document inside of the folder, named **Adminfile**. Type the following information in the file "**This information is encrypted by the Administrator**."

5. Give labuserXXa **read privileges** to this folder. (**Right click** on AdminEncrypt folder, choose **properties.** On the AdminEncrypt Properties Dialog Box, click on the **Security Tab**. Click **add**, click **advanced**, click **find now.** Look for your **labuserXXa, Highlight** the labuser and click **ok** twice. Make sure the labuser has read privileges. Click **apply** and **ok**.

6. **Logoff** as Administrator **and logon** as labuserXXa with proper password.

7. As labuserXXa, attempt to access the file **Adminfile**. Are you successful? Yes or No. Why or why not. _____

8. As labuserXXa, create a folder on the root directory named **LabuEncrypt.**

9. **Encrypt** the folder.

10. Create a file inside of the folder, name it **Labufile**. Type the following information in the file "**This information is encrypted by the LabuserXXa**."

11. **Logoff** as LabuserXXa and **logon** as Administrator.

12. Open the **AdminEncrypt** folder. **Right click** on the file **Adminfile**, choose **properties.** Click on **advanced,** click on **details.** Click on **add,** choose **labuserXXa** as someone who can read and access this file. Click ok 4 times to close the dialog box.

13. Now **logoff** as administrator and **logon** as LabuserXXa, attempt to access the file Adminfile. Are you successful? Yes or No. Why or why not.

_____

14. **Logon** as Administrator, can the administrator access the labuser's file?  Why or why not. _____

15. Local administrator can take ownership of local files.  What affect does this have in this situation?  Try a few things and be ready to discuss it.

_____

_____

**Group Policy Practical Exercise**

This practical exercise presents an overview of Group Policy and shows how to
use the Group Policy snap-in to specify policy settings for groups of users and
computers.

1. **Logon** as Administrator

2. Click **Start** ->**Run**

3. Type *gpedit.msc* and hit **Enter**

4. Under Computer Configuration, click the "**+**" next to the Windows Settings.

5. Click the "**+**" next to the **Security Settings**.

6. Click the "**+**" next to the **Local Policies**.

7. Click on the **Security Options**.

8. Double-click on the **Interactive logon: Message text for users attempting to
log on policy**.

9. In the available box, enter *Welcome to the School of Information
Technology's Systems Administration/Network Managers Security Course*.

10. Click **OK**

11. Double-click on the **Interactive logon: Message title for users attempting
to log on policy.**

12. In the available box, enter *Information Assurance*.

13. Click **OK**

14. Under Computer Configuration, click the "**+**" next to **Windows Settings** to
contract the tree.

15. Under User Configuration click the "**+**" next to **Administrative Templates**.

16. Click the "**+**" next to **Control Panel**.

17. Click on the **Display folder**.

18. Double-click **Hide Screen Saver tab**.

19. Click the **Enabled radio button**.

20. Click **OK**.

21. Double-click **Screen saver**.

22. Click the **Enabled radio button**.

23. Click **OK**.

24. Double-click **Screen saver executable name**.

25. Click the **Enabled radio button**.

26. In the Screen saver executable name box, enter ***Logon.scr***.

27. Click **OK**.

28. Double-click **Password protect the screen saver**.

29. Click the **Enabled radio button**.

30. Click **OK**.

31. Double-click **Screen Saver time out**.

32. Click the **Enabled radio button**

33. In the Number of seconds to wait to enable the Screen Saver space, enter "***10***".

34. Click **OK**.

35. Go to **File** and click **Exit** to close the Group Policy window.

36. **Logoff**.

37. Attempt to logon

38. Did the logon message appear?
    _____

39. **Logon** as the administrator

40. **Right click** on the desktop

41. Click on **properties**

42. Change your screen saver

43. Did the screen saver tab appear?

   _____

44. Wait 10 seconds

45. Did the screen saver display after 10 seconds?

   _____

46. What screen saver was activated?

   _____

**Auditing & Logging Practical Exercise**

Various steps are involved when you set up a secure server.  One of the most important is arriving at an auditing policy that does not degrade performance and meets your security needs.  By default, Windows 2000 and 2003 have auditing turned off.  In order to capture any auditing information, you must individually enable those items you wish to capture data about.  Your auditing policy will guide you as you select those events to audit.

1.  Login to the Windows Server as the administrator

2.  Click **Start**->**Run**->type **mmc**

3.  On the Console menu, click **File**, click **Add/Remove Snap-In**, and then click **Add**.
4.  In the Add Standalone Snap-In dialog box, select **Security Configuration and Analysis,** and then click **Add**.
5.  Click **Close** and then click **OK**.
6.  On the Console menu, click **File**, click **Save**.
7.  In the File Name box, type **security config & analysis** to name this console and click **Save**.
8.  On the console menu, click **exit**.
9.  To verify that the console appears on the Administrative Tools menu, click **start**->**programs**->**administrative tools**.
10. Does the security config & analysis snap-in appear as a menu item?  If no ask Instructor for assistance.
11. Choose the **Security Config & Analysis**.
12. In the Security Configuration and Analysis console, **right-click** Security Configuration and Analysis.
13. **Click** Open Database.   In the Open Database dialog box, in the File Name box, type **new** for the new personal database file name, then click **Open**.
14. In the Import Template dialog box, select the "**setup security**" security template to load into the security database, then click **Open**.  The "new" database is now the working security database, and it contains the "setup security" security template.
15. **Right click** security configuration and analysis.
16. Select "**configure computer now**".
17. Accept the default error log location by clicking "**ok**".  Close configuration and security analysis console.
18. Select **Start**->**Programs**->**Administrative Tools**->**Local Security Policy**
19. Expand **Local Policies**
20. Select **Audit Policy**.  Which policies are enabled by with this template?

You should see a column labeled security settings. In the case of inherited policies, you may see two columns, one for local security settings and one for effective settings. The local security settings pertain to settings established on the computer itself.

21. **Right click** on Audit Logon Events and select **properties**

22. Click on both **success** and **failure** and then click **ok**

23. **Right Click** on Audit Object Access and select **properties**

24. Click on both **Success** and **failure** and then click **ok**

25. **Right click** on Audit Privilege Use and select **properties**

26. Click on **failure** and then click **ok**

27. **Right click** on Audit System Events and select **properties**

28. Click on **failure** and then click **ok**

29. Close Local Security Settings window and then reopen Local Security Policy. Have your changes become effective?

_____

30. Select **Start**->**Programs**->**Administrative Tools**->**Event Viewer**

31. **Right Click** on the Security Log choice in the left panel

32. Choose **properties**

33. If you click on the filter tab you will see the various events the log looks for. You can keep the size of your log down by choosing to not filter for certain events. What events can you filter on?
_____
_____

34. **Click** on the General tab.

35. What is the default size setting?
_____

36. Change the log file size setting to **100KB** and click **Apply**. Were you successful?

37. What is the restriction when setting the log file size?  When you attempted to set the log size to 100KB, what did the system choose as a setting?

_____

_____

38. Select **OK** and close all windows

39. Logoff as the **administrato**r

40. Log on as **labuserX** but do not provide a password (just hit enter)

41. Repeat the previous step, four more times

42. Logon as **labuserXa** with the proper password

43.  Click on **Start**->**Run** and type **eventvwr.msc**

44. View the Security Log.  Were you successful?   _____

45. Close the Event viewer Window.

46. **Double click** on the time display in the lower right portion of the screen.  Will it allow you to change the time?  _____

47. Logout as **labuserXa**

48. Login as the **administrator** but do not provide a password (just hit enter)

49 Repeat the previous step, four more times.

50. Login as the **administrator** with the **proper password**

51. Click Select **Start**->**Programs**->**Administrative Tools**->**Event Viewer**

52. View the Security Log.

53. Can you identify the entries that were generated as a result of the bad login attempts, successful login attempts, and failure of privilege use?

_____

54. Right Click on a few of the failure and success audit event and view the properties.  You should see a fairly understandable explanation of the event. Compare your event id numbers to the common event id numbers in Section 6

Auditing.  Visit the website www.eventid.net to check for event ids not listed in the Auditing section.

> 55. Close the event viewer.

> 56. Wait for the instructor to review the exercise.

**Web Server Security Practical Exercise**

**Microsoft Internet Information Server (IIS) 6.0**

**Practical Exercise #1**

**NOTE:  During this practical exercise, do NOT open multiple copies of the Internet Service Manager.**

**FTP Site Security Settings**

1.  Open the **Internet Information Service (IIS) Manager  (Start->Programs->Administrative Tools)**
2.  **Click on local computer then double click on ftp sites**
3.  Select the **Default FTP Site** right click and select **Properties**
4.  On the **FTP Site** Tab. Verify that **Enable Logging** is checked, select the **W3C Extended Log File Format** and click on **Properties**
5.  Where is the default Log file directory

    _____

6.  Is this something you might want to change?  **S/NO**

7.  Why

    _____

8.  Select the **advanced** Tab
9.  Verify that **Time**, **Client IP Address**, **Method**, **URI Stem**, **Protocol Status and Win32 status** are checked. You can check other options if you would like, but do **NOT** uncheck any. Click **OK**.
10. Next select the **Security Accounts** Tab
11. Notice the IUSR_computername account, what is this for

    _____
12. Verify that **Allow only anonymous connections** is checked. Depending on how your FTP site is setup, this is the recommended method. Why would you want to force your users to log into FTP using the anonymous account

    _____
    _____

13. Next select the **Messages** Tab. In the **Welcome** window we will be adding the DOD Warning Banner.
14. Copy the warning banner text and paste it into the FTP **Welcome** window (It can be found on your CD.)
15. Next select the Home Directory Tab. Verify that **Read** is checked, **Write** is NOT checked, and **Log visits** is checked. Are these webserver or filesystem permissions

    _____

16. Next select the **Directory Security** Tab.
17. Now we will modify the **TCP/IP Access Restrictions** so that only your partner is **Granted Access** to your FTP sight.
18. Click on the **Denied Access** radio button. Click on **Add**. Select the **Single Computer** radio button and type in your partner's IP address. Click **OK**.
19. Click **OK** to close the FTP Properties Sheet.

**Connecting to the FTP Server to verify TCP/IP  Access Restrictions**

1. Any files you place into the **(Server Drive)\Inetpub\ftproot** directory will be downloadable when someone FTP's to your site, if they are given read access.
2. Begin by creating a file called **Army.txt** in the **(Server Drive)\Inetpub\ftproot** directory.  (you can add some text to the file if you wish)
3. Log onto your partners FTP site.  You can use **either** of the following methods:

**Command Line Method:**

a) Open up a command prompt
b) Type **ftp** (Partners IP Address)
c) Enter **anonymous** as the login (watch spelling)
d) You do not have to enter a password, just hit **enter**.
e) Did the DOD Login banner appear **S/NO** (If no, make sure your partner made one.)
f) Type **dir** to get a directory listing. Does **Army.txt** appear in the listing **S/NO**    (If no, make sure your partner put one in their ftproot directory.)
g) Type **get Army.txt** to copy the Army.txt file to your hard drive. (Note: the file will be copied to whatever directory you started the FTP command from.)
h) Next try to FTP into any system that has not permitted you. Are you allowed access **YES/**    (If yes, make sure the person at that system is at least this far in the PE.)

**Browser Method (If you used the above method, this is not necessary)**

a) Open up **Internet Explorer**
b) In the Address Field type **ftp://**(Your Partners IP Address)
c) The Browser will automatically enter the anonymous username & null password
d) Did the DOD Login banner appear **S/NO** (If no, make sure they made one.)
e) On the screen you should see the **Army.txt** file. (If not, make sure they put one in their ftproot.)
f) Right click on **Army.txt** and select **Copy to folder…** Keep the defaults and save the file as Army.txt in the base directory of the Server drive.

g) Next try to FTP into any system that has not permitted you. Are you allowed access **YES/** (If yes, make sure they are at least this far in the PE.)

h) Now continue to the **FTP Logging Exercise**.

**FTP Logging Exercise**
**(Note:  There will be no log file if no-one has logged into your FTP server)**

1. Open up the directory located at
(Server Drive)**\windows\system32\LogFiles\MSFTPSVC1**

2. Notice the date in the filename, it should be today's date.

3. Open the file and look at the time indicated by the entries in it. Why does it seem so off (Hint: remember, your time zone is not the primary one used by the rest of the world).

_____

___

_____

___

4. Did the logfile successfully capture the IP addresses accessing your FTP site?  S/NO

5. Does the logfile tell you whether or not the user was granted access  S/NO
(Hint: look at the three digit code)

530 = Wrong Password
230 = Correct Password

6. Does the logfile indicate filenames, if any that were sent to a user?  S/NO

7. You probably see **USER**, **PASS**, **sent**, and **QUIT** under the uri-stem. What would it mean if you saw **created** in your log file

_____

_____

8. Close the logfile, the logfile folder, and the command prompt.

**Practical Exercise 2**

**Web Site Security Settings**

Log onto your favorite web site, *select file*, select save as and save the website to (Server Drive)\inetpub\wwwroot.  Save the file name as ***default***.  This is now the website hosted on your computer.   (Select a basic page that does not contain java script and ASP scripts, because it may not display properly)

1.  Open the **Internet Information Service (IIS) Manager**
2.  Click on **local computer,** click on **websites.**
3.  Select the **Default Web Site** right click and select **Properties**
4.  What is the default TCP Port used for the Web site ____
5.  Could a user setup a renegade web server in your office on a different port? YES/NO
6.  On the **Web Site** Tab Verify that **Enable Logging** is checked, select the **W3C Extended Log File Format** and click on **Properties**
7.  Select the **Advanced** Tab
8.  Verify that **Date**, **Time**, **Client IP Address**, **Method**, **URI Stem**, **Protocol Status**, and **User Agent** are checked.  Uncheck **URI Query**.  You can check other options if you would like.  Click **OK**.
9.  Next select the **Home Directory** Tab.
10. Verify that **Write**, and **Directory browsing allowed** are NOT checked.

11. Recall what Directory Browsing allows.  In what type of setup would you allow Directory browsing
    _____

12. Next select the **Directory Security** Tab
13. Under **Authentication & Access Control,** click on **Edit**
14. What are the four types of Authentication Methods

    1. _____
    2. _____
    3. _____
    4. _____

15. Why would you use Basic Authentication instead of Integrated Windows Authentication
    _____
    _____

16. Basic Authentication is sent in Clear Text, is there a way to keep Basic Authentication from being read off the wire **YES/NO**
17. How _____
    ___

18. Cancel out of **Authentication Methods**.
19. Under **IP Address and Domain Name Restrictions** click on **Edit**
20. As you did in the FTP Lab, set access restrictions on your web site so that only your partner can gain access.
21. Click **Apply**, then **OK** to close the Default Website Properties Sheet. (If asked about Inheritance Overrides, just click **OK**.)


**Connecting to the Web Server to verify TCP/IP Access Restrictions**

1. Start by having your partner open up **Internet Explorer** and typing in your IP address in the address bar.
2. Next have someone you did not permit attempt to access your web page. If your IP Address Restrictions are set up correctly, they should not be able to access your web site.
3. If your access-list is working correctly proceed to the WWW Logging exercise.

**WWW Logging**
**(Note:   There will be no logfile if no-one has logged into your WWW server)**
1. Open up your service log at
**(Server Drive)\windows\system32\LogFiles\W3svc#**
   Find the most current log file. **[ex Year Month Day]**
2. After opening up the log file, answer the following questions: (The columns do not line up with the field names, you can count them over at the top to find out which column is which.)

   a)   at time was the web page accessed?
       _____

   b)  What was the IP of the client accessing the web page?
       _____

   c)  What HTTP method was used  cs-method column.)
       _____

   d)  Did each object on the web page require it's own GET?   S/NO

   Close the log file and folder.

**Create Virtual Directories using the following procedures:**

**1.** Highlight and right click on **Default Web Site** and select **New > Virtual directory**.  Give it an alias of **Virt1.**
   - Open "My Computer", and create a temp directory on your server drive.
   - In the Virtual Directory Wizard, use the browse button to point to the temp directory you just created
   - Allow read access
   - Allow  browse
   - Remove run scripts (such as ASP)
   - Click **Next** and **Finish**

2. Highlight default Web Site and **right click Properties,** Under **performance tab**,
   - Limit connections to 10

3. On the Web-Site tab, what port would be used if SSL was installed \_\_\_\_\_.  Click OK to close Default Website Properties screen.

4. Open Internet Explorer and in the address box type
   http://(your_IP_address)/Virt1 – the virtual directory should appear.  **Note:** If the directory does not appear, read the error message and look for the error code in it.  It will usually give you a clear reason why you aren't allowed to view the page.  Fix this problem.  Did you add your address to be able to access the site?

5. Now that you can see the Virtual Directory, add some files to it by going back to "My Computer" and placing some files in the temp directory you made earlier.  When you refresh your browser, they should appear in a list.

6. Go back to the temp directory folder and create a new text file.  Type a few lines of text in the file, and save it.  Then rename the file to **default.htm**.

7. From the Internet Explorer, hit the refresh button.  What happened?
   _____
   _____

8. Go back to the Internet Services Manager.  Right-click on your **Virt1 Virtual Directory**.  Select **Properties**.  Click on the **Documents** tab.  Notice the section labeled "**Enable Default Content Page**."  This section controls the documents that will be automatically displayed to viewers if they are present.  The documents listed are processed in order from top to bottom.  The first one it finds in the directory will be the one displayed.  This can be used as a type of safety feature to keep users from viewing directories.  Even if directory

browsing is enabled, as long as one of these files exists in a directory, the contents of that directory will not be displayed by IIS.  At the same time, the existence of one of these files can inadvertently affect directory browsing.  If you wish to show the contents of a directory that <u>does</u> contain one of the listed document files, you have to either uncheck the **Enable Default Content Page** box, or remove the necessary filenames from the list.

9.  Close the folder, Internet Explorer, and any editors you may still have open.

**Practical Exercise 3**

**Secure Socket Layer Lab**
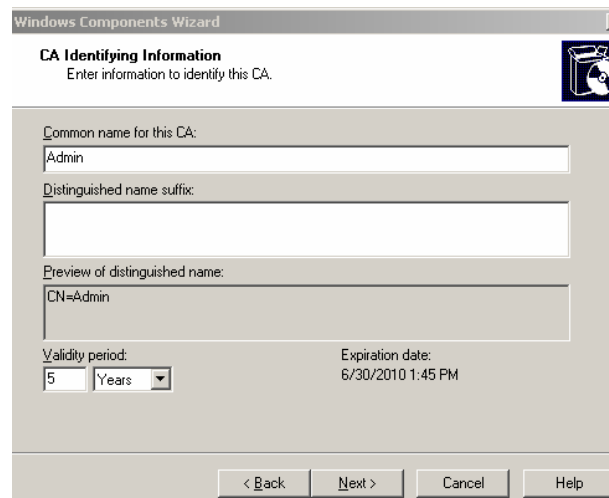
Objectives:
   I.  Setup a Certificate Authority
  II.  Request and Process a Server Certificate
 III.  Verify functionality of SSL

I.  Setting up a Certificate Authority

**Our Certificate Authority issues the keys needed to run our Public Key Infrastructure**

1.  Click **Start**, **Settings**, **Control Panel.**

2.  Double click **Add/Remove Programs**.  (Close the Control Panel)

3.  Click **Add/Remove Windows Components**.  This will start the **Windows Components Wizard**.

4.  Check the **Certificate Services** box, select **Yes** in the dialog box to continue and then click **Next**.  Once installed, the computers name, or domain can no longer be changed.

5.  The Wizard now prompts you to select the type of Certification Authority. Keep the default selection of **Stand-alone root CA**., click **Next**.  (The **Advanced Option** is used to change cryptographic settings)

6.  Next you must enter identifying information.  See Figure 1.  (You may enter anything you wish in any of the areas, but leave CA Name set to Admin.)  Then click **Next**.



Figure 1

7.  Next we need to define a location for the certificate database, configuration information, and Certificate Revocation List (CRL).  Leave the default entries. See Figure 2.  Then click **Next**..
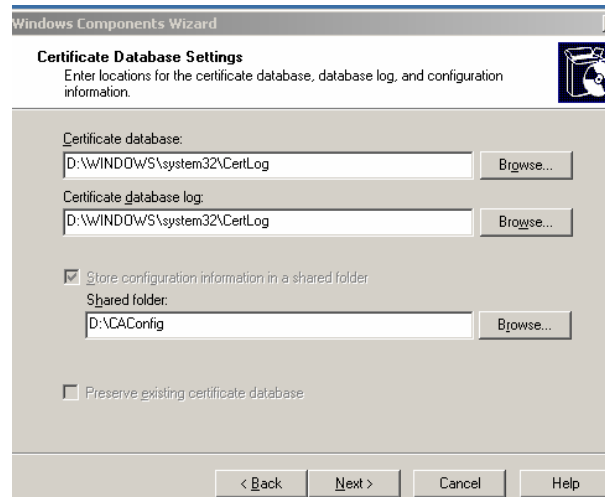
Figure 2

8. If IIS is running, a message will prompt you to stop IIS. **Click yes** to Stop IIS. This must be done in order to install the Web components.

9. If windows prompts you for some needed files, Browse or point the Wizard to the (CDROM)**:\i386** folder. You may have to insert the Windows 2003 CD. Then click **OK**. You want to enable Active Server Pages now.

10. Click **Finish** and **Close** the **Add/Remove** window.

11. Now lets verify that the Certificate Authority is installed and running:

At a Command Prompt type **net start** and scroll up to find **Certificate Services**.

If Certificate Services is not listed, contact the instructor. If it is, close the command prompt.

**II. Request and Process a Server Certificate**
We need to set up IIS with a Web Server Certificate

1. Go back to the **Internet Information Services (IIS) Manager**.

2. Right click on **Default Web Site**, then **Properties**.

3. Select **Directory Security** tab.

4. Under **Secure communications**, select **Server Certificate**.

5. In the Wizard click **Next**

6. Select **Create a new certificate**, Click **Next**

7. Then select **Prepare the request now, but send it later.** Click **Next.**

8. Type **Test Server** in the **Name** field and leave **Bit Length** at **1024**. Click **Next**

9. In the **IIS Certificate Wizard** enter the following info:

   Organization:       **US ARMY**
   Organizational unit:  **SIT**    click **Next**

   Leave Common name at default    click **Next**

   Country/Region:   **Us (United States)**
   State/province:    **Georgia**
   City/locality:     **Ft. Gordon**  click **Next**

   File name:      (Server Drive)**\certreq.txt**  click **Next**

10. Verify information is correct, click **Next**, then **Finish**

11. In the **Default Web Site Properties** window, click **OK**

12. Open IE (Internet Explorer), type  **http://(Your_IP_address)/certsrv** , Select **Request a certificate**.

13. Select **Advanced request**.

14. Select **Submit a certificate request using a base64 encoded PKCS #10 file**.

15. Find the **certreq.txt** file that you created in step 10.  Open it in Notepad (You will have to go to "My Computer" to do this), then select (highlight) __ALL__ of the text, including:

    **-----BEGIN NEW CERTIFICATE REQUEST-----**

       { *lots and lots of stuff* }

    **-----END NEW CERTIFICATE REQUEST-----**

16. Once __ALL__ of the text is highlighted, **Copy** and **Paste** it into the **Saved Request** field.  Close notepad when done.  See figure 3

    QUESTION:

    What does the *Block of the Garbage* look like? (Hint:  Peek at Appendix A)
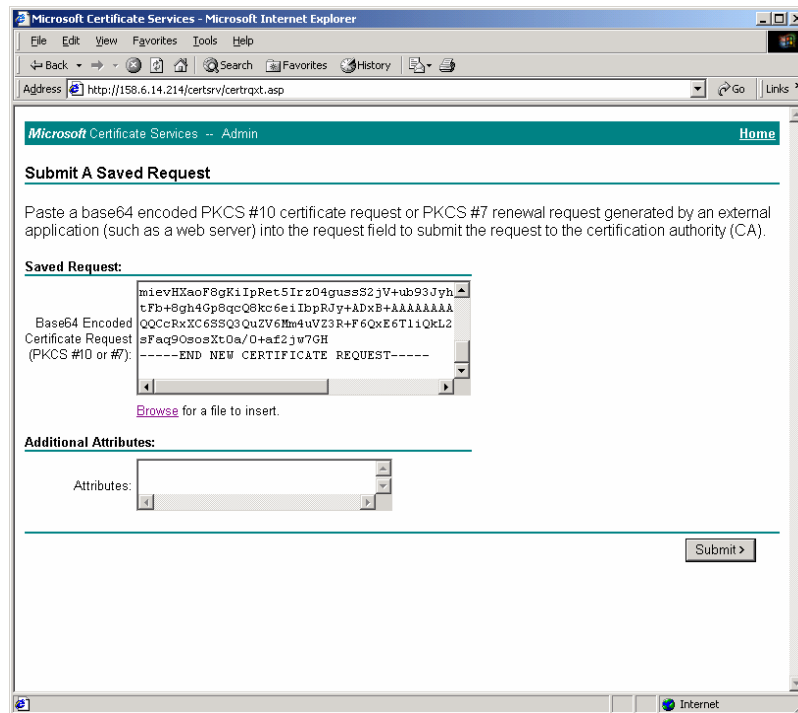
Figure 3

17. Click **Submit**

18. Notice the Certificate Pending status

**Process the Certificate we just requested.**

1. **Start**, **Programs**, **Administrative Tools**, **Certification Authority**

2. Highlight **Admin** then select **Pending Requests** folder

3. You should have one certificate pending.  Right click on the pending request, select **All Tasks**, **Issue**

4. The pending request should now be in the **Issued Certificates** folder.

5. Certificate Service must be restarted at this point.  Right-click on **Admin**, Select **All Tasks**, then click on **Stop Service**.  When it completes stopping the service, take the same steps, but click on **Start Service**.

6. In your browser (IE), type **http://(Your_IP_address)/certsrv**

7. Select **View the status of a pending certificate.**

8. Select the **Saved Request Certificate.**

9. Select **Base 64 encoded**, click on **Download certificate**.

10. In the **File Download** dialog box, select **Save**.

11. Save it on your **(Server Drive)**, leave File name: **certnew**,  click **Save.**

181

12. In the IIS (Internet Information Services) window, right click on **Default Web Site**, select **Properties**, select **Directory Security** tab, select **Server Certificate** in the **Secure communications** section.

13. Click **Next** in the **Web Server Certificate Wizard**.

14. Select **Process the pending request and install the certificate**, click **Next**.

15. Make sure the Path and file name is **(Server Drive)\certnew.cer**, click **Next**.

16. View the certificate information, click **Next**.

17. After you see the **You have successfully completed the Web Server Certificate Wizard** message, click **Finish**.

**III. Let's setup and verify the functionality of SSL**

18. Notice all of the options under **Secure communications** are now available.  Select **Edit**.

19. Check the box for **Require secure channel (SSL)**, click **OK**

20. Click **OK** on the **Default Web Site Properties** window.  (If asked about Inheritance Overrides, click OK)

21. In your web browser (IE) type **http://(Your_IP_address/**

    What response did you get?

    What can you do in order to view this page? (Remember it is a secure website now!)

    What are two indicators that you have a secure connection? (Do not count any boxes you clicked away)

    If you were presented with a dialogue box that stated that some items on the page were secure and some were not, then it asked you if you'd like to view the insecure items:  If you selected "Yes", then the lock will not display, and you should see all the items on the page.  If you selected "No", then the lock should be there, and you will see some items missing from the page.

## IIS Summary & Security Tips

1. Do not ever use the "default web" always create a brand new web in a completely different path on the hard drive if possible.

2. Do not use ANY ISAPI filters unless you MUST.

3. Remember there is a new IIS hole bound to come out at least once a month.

4. Guard yourself from the attacks that are yet to come. Basically it does not matter how many service packs or hot fixes you install there will always be that one new hole that comes out that bites you where it hurts. Remember to look for things that are out of the ordinary, you should never have a request to your website that has "/../../../../../../../" somewhere within it. There are a lot of "path attacks" against various ISAPI filters... they all have the same basic characteristics so look for patterns.

5. Consider obscurity -- Obscurity isn't good security but it is better than using defaults. There is nothing wrong with not installing software in their default directories to foil script kiddies or the easily discouraged hacker. Don't save orders to orders.txt. Don't put logs in a directory named logs. With so many other sites for a hacker to hack sometimes a little obscurity can be enough to save you.

6. Your site is never secure -- Don't brag about how secure your site is on your privacy page. Don't even mention how secure you are because you will start believing it yourself and let your guard down.

7. Training is the key for web administrators/developers. They should be able to test their own content. If not get signed up for more training.

   a) HTML 4/ XML / HDML / C / C++ / Visual Basic / Active X / Java / Perl

8. Purchase the Internet Information Server Resource Kit and read the chapter on Security.

**Network Monitor Practical Exercise**

1.  Execute the Network Monitor by clicking on **Start --> Programs --> Administrative Tools --> Network Monitor**

2.  At the Microsoft Network Monitor message block, click **OK**

3.  At the "**Select a network**" box, expand the "**Local Computer**"

4.  Select **Local Area Connection** and click **OK**

5.  Maximize your network monitor screen

6.  In the tool bar at the top of the screen, click the funnel (filter shaped)
    *This will allow us to edit the capture filter*

7.  An information box pops up. Please read it and click **OK**

8. In the Capture Filter window select **[Address Pairs]** (**by double clicking**)

9. In the **Address Expression** set the filter to include **ANYGROUP  <---> ANY**
    *This allows us to include and exclude entries for detection from station to station. It also allows us to control the directional flow of data we detect.*

10. Can we set the filter to only capture outgoing broadcast traffic from the local host?  If so how could we do this?

11. Click **OK**

12. You can click **OK** to exit out of the Capture Filter window.

*We will now capture all traffic going to or coming from this machine to include*

*general broadcasts*

**Capturing Network Traffic**

1. In the tool bar at the top of the Network Monitor screen, click on the ICON shaped like the play button on a VCR. *This will start the network capture*

2. After allowing the Network Monitor to run for two minutes, press the stop ICON.

3. Click on the eyeglass ICON in the toolbar to view captured data.

**IV. Analysis:**

   1. Which protocol was the most common?

   2. What was the most common Source MAC Address?

   3. What was the most common Destination MAC Address?

   4. By clicking on **Display** ---> **Colors** set the most common protocol to be a different color than the rest, click **OK**. How can changing the color scheme on certain protocols be beneficial to the administrator?

   5. Take a closer look at the Ethernet Frame. Double Click on one of the Frames in the list. If a password were sent across the network in clear text, in your opinion would it be viewable by the Network Monitor?
                                    Yes / No

**Clear Text Vulnerability**

Working with your partner, we will examine clear text vulnerability and how to utilize IP Security to counteract this vulnerability. You will change the filter to only capture traffic between your and your partner PC's.  You will then Ping, FTP, and Telnet to each other PC.

**\*\* Please stay in sync with your lab partner**

   **Both Users**

   1. From menu at the top of the screen - Select **Window** then the **– Local Area Connection Capture Window** – session

   2. Click on the **Funnel** icon

   3. Double Click **INCLUDE \*ANY GROUP < -- > \*ANY**

   *Now we will add in our partner PC*

   4. Click **Edit Addresses.**

   5. In the Address Database, select **Add.**

   6. Enter Partner PC name – **w2k3xxx** (xxx is the last octet of IP)

   7. Change **Type** to **IP**

   8. Enter your Partner PC IP address in the **Address Block**– **147.51.217.xxx** (xxx is the last octet of IP)

   9. Select **OK**

   10. In the Address Database, click **Close**

   11. Set the filter to w2k3XXX (your machine name) <--> w2k3xxx (your partner pc)

   12. Select **OK**

**Now we will only capture packets between our two machines**

*The filter should look like **Your machine name(IP) < -- > Your partner PC(IP)***

   13. Select **OK** to close the Capture Filter window

**\*\*Don't continue with this PE until you and your partner have completed the previous steps.**

*PING session*

1. **<u>Both Users</u>**

2. Click the **record** button to start the recording session

3. **<u>One of the users</u>** - Open a command prompt – **start** – **run** – type **cmd**

4. Ping your partner PC – type **PING 147.51.217.xxx**

5. Once the Ping has finished – stop the capture

6. View what has been captured

7. What did we capture?

8. Double click the frame.  In the detail pane (second pane), click the "+". What is your ICMP data?

*FTP session - We will now FTP from one box to the other*

<u>Both Users</u>

1. From menu at the top of the screen - Select **<u>Window</u>** then the **– Local Area Connection Capture Window** – session

2. Click the **record** button to start the recording session

3. **<u>One of the users</u>** - **start** – **run** – **cmd**

4. Enter **ftp 147.51.217.xxx** (partner PC)

5. Enter **administrator** as user and **student** as password

6. At the ftp> enter **bye**

**Both Users**

7. Stop the capture

8. View what has been captured

9. Did you capture the username and password?

**Both Users**

1. From menu at the top of the screen - Select **Window** then the **– Local Area Connection Capture Window** – session

2. Click the **record** button to start the recording session

3. **One of the users** - Click – **start** – **run** – **cmd**

4. Enter **telnet 147.51.217.xxx** (partner PC)

5. Enter **administrator** as user and **student** as password

6. Type **dir**

7. Type **cd** (find a directory to change to)

8. Type **dir**

9. Type **Exit**

    **Both Users**

10. Stop the capture

11. View what has been captured

12. Did you capture the username and password?

13. How is Telnet different from FTP, look very closely?

14. What are some things we can we do to protect our selves from clear text vulnerability?

**IPSEC Practical Exercise**

This practical exercise will provide hands-on training using Internet Protocol
Security (IPSec) to encrypt network traffic.  IPSec provides the ability to
authenticate and encrypt network connections between two computers.  You will
need to synchronize your steps with your PARTNER on another machine.  This
practical exercise will be performed in Windows Server.

**Creating a Custom Management console for local IPSec**

1.  Click **Start**->**Run**->type **mmc**
2.  On the Console menu, click **File**, click **Add/Remove Snap-In**, and click
    **Add**.
3.  In the Add Standalone Snap-In dialog box, select **IP Security Monitor**
    and **IP Security Policy Management** (on local computer), and click **Add**
    for each.
4.  Click **Close** and then click **OK**.
5.  On the Console menu, click **File**, click **Save**.
6.  In the File Name box, type **IPSEC** to name this console and click **Save**.

**Creating a IPSEC Policy**

7.  **Highlight** and **right click** on **IP Security Policies** on local computer.
8.  Select **Create IP Security Policy**
9.  When the IPSec Policy wizard appears, click the **Next** Button.
10. In the name box type **IPSEC Custom1**, in description box type
    **Information Assurance** and click the **NEXT** button.

*Note:  The Requests For Secure Connection page appears*

11. Verify that the Active Default Response Rule check box is **selected**, click
    **NEXT.**
12. Accept default response, (Kerberos Rule Authentication Method Box) click
    **NEXT**.

13. Click **Yes** to the warning.

14. Leave the Edit Properties check box selected, click **Finish** Button.

15. **Clear** the Use Add Wizard in the newly created IPSec Custom1 properties Box.

16. In **Rules** tab of properties dialog box, click **Add** button.


## Configuring Filters between the two computers

**Note:  You will be configuring filters between your computer and your partner's computer**. One student will be Workstation #1 and the other will be Workstation #2.  Instructor will designate partners.

1. Click the **Add** button in the IP Filter List tab.

    a. Workstation #1

        i. In IP Filter List pane, highlight and rename the filter to **CustomFilter1 Host A to B**.

    b. Workstation #2

        i. In IP Filter List pane, highlight and rename the filter to **CustomFilter1 Host B to A**.


2. Perform the following at Both Computers.

3. **Clear** the Use Add Wizard check box.

4. In Ip Filter list tab, click **Add** button (IP Filter Properties box appears).

5. In *Source Address*, select **A Specific IP address**.

6. Input your **ip address**.

7. In the *Destination Address*, select **A specific IP Address.**

8. Input **your partners IP address**, click **OK** twice.

9. In IP Filter List tab, select **CustomFilter1** option (Fill in the radio button).

Next task is to configure input and output Filter Action:

Note:  Filter Action specifies what security action will take place upon starting a filter.  The action specifies whether to permit the traffic, block the traffic, or negotiate the security for the given connection.  In addition, additional settings are available to react if non-IPSec protected data is received.

10. Open Filter Action tab, **clear** the Use Add Wizard check box, and then click **add**

11. On the Security Methods tab, click **Add.**

12. In New Security Method dialog box, select **Custom** option, click on **settings**, check **Data and address integrity without encryption (AH)**, deselect **Data integrity and encryption (ESP),** then click **OK** twice.

13. New Filter Action Properties dialog box, open **General tab.**

14. In the Name box, type **Authentication Header**, then click **OK.**

15. Select the **option** button next to **Authentication Header** (Fill in the radio button).

16. Open **Authentication Methods** tab.

17. Click **Add** button.

18. The new Authentication Method Properties dialog box appears.

19. Select the **Use This String** (preshared key). Fill in the radio button.

20. On the New Authentication Method properties dialog box, in the **Use This String** area, type **informationassurance** in the text box, click **OK**.

21. Select *__Preshared Key__* in the list, <u>click</u> the **Move Up Button**.

22. Click **Close** to return to the IPSEC Custom1 Properties dialog box and to complete the creation of this rule.

23. Click **OK** in the IPSE Custom1 Properties dialog box to close.

**Testing a Custom Policy**

**Note: Ensure you and your partner are working together.**

24. Assign the policy just made (IPSec Custom1).

25. In right pane of custom console, **right click** the IPSec Custom1 policy, click **assign.**

26. The policy Assigned column value is set to **yes**.

27. Configure the IPSec Monitor and review IPSec statistics.

**Configuring IPSec Monitor**

28. At the IPSEC Console Window Screen, highlight IP Security Monitor. Your computer name should be present.

29. **Right click** on IP Security Monitor, choose **Add computer**, input your partner's workstation name (w2k3xxx), and then click **OK**. You should now see both your computer and your partner's computer on your console under IP Security Monitor. **Double click** on your partner's computer. It may take a while, but you should see a green arrow on your partner's computer. This will prove that your systems have created an association between the two.

30. Under IP Security Monitor, click on the **+** beside your computer to expand the options. Click active policy to view information about your current policy. Continue to view all the modes and filters.

At this point, both users should have Network Monitor, IP Security Monitor and IP Security Policies on local computer available.

31. *PING* your partners computer
    a. The first ping may fail due to time it takes to negotiate the policy. (If the green arrow shows up on both systems under the IP Security Monitor, your ping will not fail because the policies will have already been negotiated.)
    b. With matching policies on both computers, future **pings** should work.
    c. Alternatively, enable and disable the policy to see the effects of non-matching policy settings.

    Note: In IP Security Monitor, you will see a green arrow on both systems showing your polices are associated. The IP Security Monitor will allow

you to see the policy name, security, filtername, src address, dest address, protocol, src port, dst port and tunnel equipment.

32. Stop !!! and review information.

## To view IPSEC integrity packets (Authentication Header)

33. Start **Network Monitor** and if not set from previous Practical Exercise set the **capture network** to the appropriate media access control address network card.

34. Make sure the IPSec Custom1 policy is assigned.

35. Start capturing packets w/ Network Monitor.

36. *Ping* second computers IP address.
    Note: may have to repeat because PING has a short time-out, and the delay establishing IPSEC association between two computers.

37. Stop and view the capture on NETMON.

38. **Double-click** the first Internet Control Message Protocol (ICMP) packet. The capture window will be broken into three separate sections (Frames, Protocols and detailed information ASCII and Hexidecimal).

    **Note**:  You should see headers fo*r frame, Ethernet, IP, AH* and ICMP in detailed pane.

39. Expand **IP entry** and record IP Protocol name
    _____.

40. Expand **ICMP entry** and record Number of Data Bytes remaining
    _____.

41. Notice IP payload is in clear text.

42. The data for a PING is _____.

**Now we will initiate FTP and Telnet connections utilizing IPSec.**

43.  Open a command prompt (Click **start** – **run, type cmd).**

44. At the command prompt enter **ftp xxx.x.xxx.xx** (partner PC).

45. Enter **administrator** as user and **student** as password.

46. Type **bye.**

47. Next open command prompt **(**Click **start** – **run, type cmd)**.

48. At the command prompt enter **telnet xxx.x.xxx.xx** (partner PC).

49. Enter **administrator** as user and **student** as password.

50. Type **exit.**

Now let's see if we can see our user and password information

51. **Both Users**

52. Stop the capture

53. View what has been captured

54. What did we capture for FTP and Telnet?  Can you locate the User name and password?

**55.** What protocols did we pick up?

***To set higher encryption:***  *By configuring Integrity Only (Authentication Header AH) method, we ensured authentication but did not encrypt the data in the packet.  AH just makes sure that the packet data, as well as mot parts of the IP header, source and destination IP addresses, are not modified.  We will now look at traffic using the ESP security method that will encrypt the data part of the IP packet.*

56. **Right-click** IP Security Policies on Local Machine.

57. Click **Manage IP Filter Lists and Filter Action**.

58. Click **Manage Filter Action tab**.

59. Select **Authentication Header**.

60. Click **edit**, twice.

61. In the edit Security Method dialog box, click on **settings**.

62. On the Custom Security Method Settings box, deselect **Data and address integrity without encryption (AH)**, check **Data integrity and encryption (ESP),** for Integrity algorithm choose **MD5** and choose **3DES** for encryption algorithm.

63. Click **OK** three times.

64. Un-assign and re-assign the IPSec Custom1 Policy.

**View IPSec encrypted (Encapsulation Security Payload) Packets.**

65. Begin capturing packets with Network Monitor

66. *Ping* your partners computer IP address. Note: you may have to repeat because PING has a short time-out, and the delay establishing IPSEC association between two computers.

67. *S*top and view the Network Monitor.

68. **Double-click** the first ESP frame.

69. The four entries in the details pane are: Frame, Ethernet, IP, and ESP:SPI
IPSEC has created a hash of the ICMP and Data fields of the frame.

70. Expand the IP section and record the IP Protocol name

_____.

71. Scroll to the bottom of the ESP details and click the ESP:SPI
Data: Number of Data Bytes Remaining will vary but you will see **the data has been encrypted**. Look at the Hex pane; you will see the data has been encrypted instead of results of when the IP Payload was in clear text.

72. By configuring the ESP Security Method the data part of the IP packet was encrypted where as by just configuring AH security we all ensured authentication of the packet was ensured.

FINISHED !!!!!!!!!!!!!!!!!!!!!!!!

**Harris Stat Scanner Practical Exercise**

**Part 1**

This practical exercise will provide hands-on experimentation with the STAT
scanner. On the system please logon local as the Administrator and perform the
following:

Check for vulnerability on your local machine.

1. Start the STAT application. Double click on the **STAT icon** on your
desktop.

2. **Close** the read me screen if it is displayed.

3. **Close** tip of the day screen if it is displayed.

4.  Change the configuration:

   a.  Select **Configuration**

   b.  **Load configuration from file**

*This open display allows you to select various types of categories to
examine or autofix.*

   c.  Select **IE.dat**

   d.  Click on open

*On your STAT main screen, the configuration File should now read IE.dat
(Upper left corner.)*

5.  Perform an Analysis

   a.  From the console menu select **Analysis**

   b.  Click **Perform an Analysis** or select the **red sign wave icon** on
       your toolbar.

   c.  At the "Scan Ports & Services Screen, leave defaults and press
       **scan**.

d. Click **ok** on warning banner. Note: If IE6 is installed with all hotfixes no vulnerabilities should be found. Faults will be found in the right window. For classroom purposes, **DO NOT FIX THE ID# W0064 "FAT FILE SYSTEMS EXISTS."** It is needed for our Ghost version.

6. **Close** the Ports, Banners, and Services Reports and the Scan Summary report.

7. Change the configuration file setting to **C2.dat**

8. Click **Open and perform an analysis**.

9. The Replace/Append dialog box will appear. Click **Replace.**

10. Review the vulnerabilities.

11. Change the configuration file setting to **all.dat**.

12. Click **Open and perform an analysis**.

13. The Replace/Append dialog box will appear. Click **Replace.**

Note: Your machine should display numerous vulnerabilities. Scan down the list and locate ID # W0064 and W1210. (if not there, pick a couple others)

14. What type of vulnerability does it display?

_____

15. Could this vulnerability be auto fixed?

_____

Scan other machines in your subnet.

16. From the STAT scanner main screen select

a. Click on **Machines**

b. Click on **Select Machines**

c. The Machine list menu will be displayed. Ensure the block "**Automatically Test for Admin Rights**" is selected.

     d.  Click **Find Machines To Scan**

17. Select: **IP Range Selection**

18. Starting IP Address **147.51.217.xxx**  (Instructors will inform of IP Addressing scheme for each site)

19. Ending IP Address 147.51.217.xxx

20. Click on **Next**. (Standby while your computer does a search)

21. Select the **two computers** that are now present on the Machine Selection

22. Click on **Next.**

23. Click **Finish.**

24. Click **Save.**

25. Click **Close.**

26. From the STAT scanner main screen: **Highlight** one computer **hold down** the **shift key** and **select** the other computer.

27. Perform an analysis using the steps you learned above. Use the **all.dat.**

*You should see all of the vulnerabilities that the scanner performed on the machines on the right pane.  You could also select each machine from its tab on the bottom and examine each machine's vulnerability*

28. **Take ten minutes** to view some of the vulnerabilities that were found by the STAT scanner.

29.  Wait for instructor review.

**Part 2    Creation of custom IAVA configuration files**

The IAVA numbers are available in the configuration editor.  This allows you to
more easily create a custom IAVA scan file.
Perform the following steps:

1. **Open** STAT Scanner

2. Select **Configuration**

3. Select **New Configuration**

4. On the left hand side of the editor under Available Checks, **scroll to the right** and find the **ACERT IAVA ID** tab.

5. Click on the **top of the column** to sort the **ACERT IAVA ID**

6. Select the desired IAVAs and click the [>>] button

7. Click **save** and give it the file name IAW LSOP

8. Click **save**

9. Click **close**

10. Select **Load Configuration from file**

11. **Select** the newly created file

12. In the Configuration File window verify that the correct file name is loaded

13. Perform an analysis

14. Review the vulnerability results, Scan Summary, and Port and Services
    Report.

**Let's look at the procedures to run a single scan that will verify if your
Anti-Virus DAT files are out of date and then create a custom
configuration DAT file:**

15. **Open** STAT Scanner

16. Select **configuration**

17. Select **new configuration** (the configuration display will appear)

18. From the Available Checks window of the configuration display, select the following vulnerabilities by clicking on it with the mouse. (hint: hold the ctrl key to select multiple vulnerabilities at once and look in the Category Column for Anti-Virus):

    a. W1142 McAfee (Network Associates)    Medium
    b. W1986 Norton (Symantec)         Medium
    c. W1999 Trend (PC-cillian)

19. Also add to the new custom configuration file:

    a. W1983 Spyware Detection
    b. W1985 Warning Network/Monitor Sniffer
    c. W1798 LastLogon username
    d. W0084 Warning Banner
    e. W1220 Warning Banner

20. The vulnerabilities selected will be moved to the selected check column. If you accidentally added a check by mistake remove by selecting << option.

21. Click **save** and give it a file name IAW LSOP

22. Click **close**

23. Select **Load Configuration from file**

24. **Select** the newly created file

25. **Scan** your network

26. Wait for instructor review.

**Retina Scanner Practical Exercise**

This practical exercise will provide hands-on experimentation with the Retina scanner. On the system please logon local as the Administrator and perform the following:

1. Check for vulnerabilities on your local machine.

2. Start the Retina application. Double click on the **Retina5017Demo** icon on your desktop.

3. At the Welcome to eEye Digital Security Retina Demo Installation Wizard, click **Next**.

4. At the License Agreement Screen, click **Yes** to accept this agreement.

5. At the Destination Folder Screen, click **Next** to accept the destination location.

6. At the Select Additional Tasks Screen click **Next**, leave boxes checked.

7. At the Ready to Install Application Screen, click **Next** to start installation, updating system screen will appear.

8. At the Retina has been successfully installed screen, **remove the check** at Go to Windows Update Site and click **Finish**.

9. A Welcome to Retina Screen will appear if properly installed. This welcome will help you get started in using Retina.  Continue through the Welcome to Retina and click **Finish** at the end.

10. **Maximize** the Retina Network Security Scanner Window.

11. Click on the **Discover tab**.  Under the Discover tab, click on **options.** Make sure all boxes are **checked**.

12. Click on **Targets**.  Under the Target type choose **IP Range**. Choose the IP Range of 147.51.217.xxx to 147.51.217.xxx. (The xxx should be the last octet of the 1$^{st}$ computer in the class and the last computer in the class. Instructor will inform the class of the octets.)

13. Click on **Discover** to discover all systems on the network.  Wait for **Scan is completed** to show at the bottom left-corner of the screen.

14. Under Results, **right-click** on your computer IP Address and select **scan selected item**. (This will take you to the Audit Tab.)

15. On the left side of screen, under Audit Task, select **Manage Credentials**.

16. Click **Yes** on the Retina Warning Widows.

17. In the username block, type **Administrator**.

18. In the Password block and the Confirm Password block, type **student**.

19. In the Description block, type **Windows**.

20. Click **Add**.

21. Click **Close**.

22. Under Actions on the Audit Tab, click on **Ports**.

23. Ensure that only **Common Ports** is checked.

24. Under Actions on the Audit Tab, click on **Audits**.

25. Ensure that **All Audits** is checked.

26. Under Actions on the Audit Tab, click on **Options**.

27. Under Select Options, check **Enable Connect Scan Mode**, **Enable Force Scan & Randomize Target List**.

28. Under Actions on the Audit Tab, click on **Targets.** In the Job Name block, type **1$^{st}$ Scan**.

29. In the Credential block, select **Windows.**

30. Under Actions on the Audit Tab, click on **Scan**.

31. Wait until scan is complete shows in the lower left side of screen.

32. When scan is complete, change the Job Name to **2$^{nd}$ Scan**.

33. In the Credential block, choose **Null Session**. In the Addresses block, type your partner's IP address.

34. Under Actions on the Audit Tab, click on **Scan.**

35. Click **Yes** on the Retina Warning Window.

36. After the scan is complete, under the section of Scan Jobs, click on **Completed.**

37. Review the 1$^{st}$ and 2$^{nd}$ Scans. Are there any differences between the two scans?  Yes or No.  (Check closely to see if there are differences with the

Users Section and why?)

_____

38. **STOP!!!!** Wait for Instructor to review.

39. Click on the **Remediate tab**.

40. Under Scan Jobs, click on **completed**. Highlight the **1st Scan**.

41. Click **Generate** to generate a list of vulnerabilities to remediate.  (Under the configuration section, there are various filters and options to choose. Review those filters and options.)

42. Once the remediation report is completed, review the various vulnerabilities.  In this report you will see risk level, category, description, how to fix, related links, common vulnerability exposures, information assurance vulnerability and affected machines.

43. **STOP!!!**   Wait for Instructor to review.

44. Click on the **Report Tab**.

45. Under Configuration, click on **options**.  In the Report Created By box, type **System Administrator**.  In the Report Created For, type **RCERT.**

46. Under Scan jobs, click on **completed**.

47. Highlight the **1st Scan**.

48. Under Configuration, click on **Generate**.

49. Review the report that has generated.  There are many things that can be added to a report. Take a look under configuration at the sections area. Charts may also be added to your report.

50.  The report may also be saved, printed and viewed in a different context. On the left of your screen, under Report Tasks, click on **View in a Web Browser**. Continue to review the report.

51. **STOP!!!** Wait for Instructor to review.

**Security Configuration and Analysis Practical Exercise**

In this lab you will access the Security Configuration and Analysis console, set a working security database, analyze system security, and then view the results. The Security Configuration and Analysis tool offers the ability to configure security, analyze security, view results, and resolve any discrepancies revealed by analysis. This tool is located on the Security Configuration and Analysis console. This lab shows you how to use the Security Configuration and Analysis console.  For more clarification, see the Additional Info section, which follows the PE. Please perform the following steps on **Windows 2003 Server**.

**Accessing the Security Configuration and Analysis Console**
In this exercise you access the Security Configuration and Analysis console, the main tool for using the Security Configuration and Analysis tool.

**Part 1**
**To access the Security Configuration and Analysis console**
1. Click Run, type mmc, and then click OK.
2. On the Console menu, click File, click Add/Remove Snap-In, and then click Add.
3. In the Add Standalone Snap-In dialog box, select Security Configuration and Analysis, and then click Add.
4. Click Close, then click OK.
5. On the Console menu, click File, click Save.
6. In the File Name box, type security config & analysis to name this console and click Save.
7. On the console menu, click exit.
8. To verify that the console appears on the Administrative Tools menu, click start->programs->admintools.
9. Does the security config & analysis snap-in appear as a menu item?

_____
_____
_____

**Setting a Working Security Database**

In this exercise you determine the working security database to use.  To set a working security database

1. Click Start->Programs->Admintools->Security Config & Analysis.
2. In the Security Configuration and Analysis console, right-click Security Configuration and Analysis.
3. Click Open Database.
4. In the Open Database dialog box, in the File Name box, type **new** for the new personal database file name, then click Open.

5. In the Import Template dialog box, select the "securedc" security template to load into the security database, then click Open.

The "new" database is now the working security database, and it contains the "securedc" security template.

**Analyzing System Security**
In this exercise you analyze system security, comparing the settings in the security template securedc with the security settings currently running on your system.  To analyze system security

1. Right-click Security Configuration and Analysis, then click Analyze Computer Now.
2. In the Perform Analysis dialog box, verify the path for the log file location, then click OK.  (accept the default location)
3. The different security areas are displayed as they are analyzed.

**Viewing Security Analysis Results**
In this exercise you view the security analysis results.  To view security analysis results

1. In the Security Configuration and Analysis console (left panel), expand Security Configuration and Analysis.
2. Expand the Account Policies node, then click the Password Policy security area.
3. In the details pane, what is indicated in the Policy column?  In the Database Setting column?  In the Computer Setting column?

_____
_____
_____

4. In the Policy column, what does the red X indicate? What does the green check mark indicate?  What would the absence of an icon indicate?

_____
_____
_____

5. Continue to read the additional information listed on the new few pages after that wait for instructor review.

**Additional Info:**

---

**How the Security Configuration and Analysis Console Works**

---

The Security Configuration and Analysis console uses a database to perform configuration and analysis functions. The Security Configuration and Analysis database is a computer-specific data store. The database architecture allows the use of personal databases, security template import and export, and the combination of multiple security templates into one composite security template that can be used for analysis or configuration. New security templates can be incrementally added to the database to create a composite security template; overwriting a template is also an option. You can also create personal databases for storing your own customized security templates.

**Security Configuration**
The Security Configuration and Analysis console can be used to configure local system security. Through its use of personal databases, you can import security templates created with the Security Templates console and apply these templates to the GPO for the local computer. This immediately configures the system security with the levels specified in the template.

**Security Analysis**
The state of the operating system and applications on a computer is dynamic. For example, to enable immediate resolution of an administration or network issue, security levels may occasionally be required to change temporarily. After this security requirement is finished, the temporary change may not be reversed. This means that a computer may no longer meet the requirements for enterprise security.
The Security Configuration and Analysis console allows administrators to perform a quick security analysis. In the analysis, recommendations are presented alongside current system settings, and icons or remarks are used to highlight any areas where the current settings do not match the proposed level of security. Security Configuration and Analysis also offers the ability to resolve any discrepancies revealed by analysis.
Regular analysis enables an administrator to track and ensure an adequate level of security on each computer as part of an enterprise risk management program. Analysis is highly specified and information about all system aspects related to security is provided in the results. This enables an administrator to tune the security levels, and most important, to detect any security flaws that may occur in the system over time.

**Using Security Configuration and Analysis**
    A. The tasks for using Security Configuration and Analysis are
    B. Accessing the Security Configuration and Analysis console

    C.  Setting a working security database
    D.  Importing a security template into a security database
    E.  Analyzing system security
    F.  Viewing security analysis results
    G.  Configuring system security
    H.  Exporting security database settings to a security template

**Viewing Security Analysis Results**
The Security Configuration and Analysis console displays the analysis results organized by security area with visual flags to indicate problems. For each security policy in the security area, the current database and computer configuration settings are displayed.

In the details pane, the Policy column indicates the policy name for the analysis results, the Database Setting column indicates the security value in your template, and the Computer Setting column indicates the current security level in the system.

- A red X indicates a difference from the database configuration.
- A green check mark indicates consistency with the database configuration.
- A "?" means that the item defined is not on that system.
- No icon indicates that the security policy was not included in your template and therefore not analyzed.

**Part 2 Security Configuration and Analysis Practical Exercise**

This PE provides the student with familiarity with the security database and templates snap-in.  The student will learn the relationship between the security database settings and the current computer settings and how you can modify settings in the current security database directly, by modifying templates, and by importing templates.

1. Click Start->Programs->Administrative Tools->Security Config & Analysis.
2. In the Security Configuration and Analysis console, right-click Security Configuration and Analysis.
3. Click Open Database.
4. In the Open Database dialog box, select the "new" personal database file, then click Open.   The "new" database is now the working security database, and it contains the "securedc" security template.
5. Right-click Security Configuration and Analysis, then click Analyze Computer Now.
6. In the Perform Analysis dialog box, verify the path for the log file location, then click OK.  (accept the default location)
7. Expand Security and Configuration Analysis and Account Policies, then click the Password Policy security area.
8. Are there places where the Database Setting column differs from the Computer Setting column?

    _____
    _____
    _____

9. Expand local policies and click on audit policy.  Are there differences between the database setting and the computer setting?

    _____
    _____
    _____

10. Click on user rights.  Are the computer settings more stringent than the database setting?

    _____
    _____
    _____

11. Expand event log.  Click on settings for event log.  What is the value for the database security log size?   What is the value for the computer security log size?

_____

_____

12. Right click security configuration and analysis

13. Select "configure computer now".

14. Accept the default error log location by clicking "ok".

15. Right click on "security configuration and analysis" and select "analyze computer now".

16. Accept default location and select "ok".

17. Expand account policies and click on password policy.

18. Do the database settings and the computer settings differ now?.
_____

19. Expand local policies and click on audit policy.

20. Do database settings and the computer settings differ now?

_____

21.  Click on user rights.  Have the settings changed at all?  Does the computer update the policy on the computer if the database does not define it?

_____

_____

22. Expand event log and click on settings for event log.  What is the computer setting value for the size of the security log?  How does it compare to the database setting?

_____

_____

23. Go to account policies and click on password policy

24. Double click on "minimum password age"

25. Click the Define This Policy In The Database check box to allow editing, if not selected

26. Enter a new value of 20 for the minimum password age value. then click OK. This will change the value in the database.

27. Click on account lockout policy

28. Double click on account lockout threshold.

29. Click the Define This Policy In The Database check box to allow editing.

30. Set invalid login attempts to 3 and click OK.

31. Click OK on the Suggested Value Change Window.

32. Take a couple of minutes and double click on some other policies and see how easy it is to modify their value.

33. Right click on security configuration & analysis.

34. Select configure computer now.

35. Accept the default error log location by clicking OK

36. Right click on security configurations & analysis.

37. Select analyze computer now.

38. Accept the default error log location by clicking OK.

39. Expand account policies and click on password policy.  Has the minimum password age changed on the computer settings?  Click on account lockout policy.  Has the account lockout threshold changed to match the database value?

 _____
 _____

40. Right click on security configuration & analysis

41. Select "export template"

42. In the export template to box, type **new** for the file name and click on save.

43. Close the Security Configuration & Analysis window

44. Select Start->Run , type mmc and hit enter

45. In the console menu, select file, select add/remove snap-in

46. Select add

47. Select "security templates" and click add

48. Click close and then OK

49. In the console menu choose "save as"

50. In the file name block, type **security templates** and click save

51. Close console window, if asked to save, choose no.

52. Select Start->Programs->Administrative Tools->security templates

53. Expand security templates

54. Expand  \Windows\Security\Templates

55. Expand new.  If you expand and look at the policy values, you will see they match the ones you just configured in the database.

56. Expand account policies

57. Select password policy

58. Double click "maximum password age"

59. Click the Define This Policy In The Database check box to allow editing.

60. Set the password to expire in 150 days and click OK

61. Right click on "new" and choose save.

62. Close the security templates window but do not save settings

63. Select Start->Programs->Administrative Tools->security configuration & analysis

64. Right click on security configuration and analysis and select "open database".

65. Select "new" and hit enter.

66. Expand account policies and select password policy.

67. Did the maximum password age value change?  What is the value for both the database and the computer ?

_____

68. What does this tell you about editing an exported template?

_____

_____

69. Right click on security configuration & analysis

70. Select "export template"

71. Enter **new1** as the file name and click save

72. Select Start->Programs->Administrative Tools->security templates

73. Expand security templates

74. Expand /Windows/Security/Templates

75. Expand new1

76. Expand account policies and click on password policy

77. Double click maximum password age

78. Click the Define This Policy In The Database check box to allow editing.

79. Set the password to expire in 90 days and click OK

80. Right click on new1 and select save.

81. Close the security templates window and if asked to, do not save

82. Select the security configuration & analysis window and right click on security configuration & analysis

83. Select import template.

84. Select "new1" and click open

85. Expand account policies and select password policy

86. Has the maximum password age changed for both the database and computer value?  what is the current value?  What does this tell you about importing templates?

_____
_____
_____

87. Close all windows.

88. Continue to read additional Information and wait for instructor review

**Additional Info:**
**Configuring System Security**
Security Configuration and Analysis offers the ability to resolve any discrepancies revealed by analysis, including the following:

- Accepting or changing some or all of the values flagged or not included in the configuration if you determine the local system security levels are valid due to the context (role) of that computer
- Configuring the system to the original database configuration values if you determine the system is not in compliance with valid security levels
- Importing a more appropriate template, for the role of that computer, into the database as the new database configuration and applying it to the system
- You can repeat the import process and load multiple templates. The database will merge the various templates to create one composite template, resolving conflicts in order of import; the last one imported takes precedence when there is contention. Once the templates are imported to the database, you can choose Configure System Now to apply the stored template (database configuration) to the system.

**IMPORTANT**

These changes are made to the stored template in the database, not to the security template file. The security template file will only be modified if you either return to Security Templates and edit that template or export the stored configuration to the same template file.

**Security Templates Snap-In**
A security template is a physical representation of a security configuration; it is a file where a group of security settings may be stored. Windows 2000 includes a set of security templates, each based on the role of a computer. The templates range from security settings for low security domain clients to highly secure domain controllers. They can be used as provided, modified, or serve as a basis for creating custom security templates.

**Using the security Templates Snap-In**
A security template is a physical file representation of a security configuration, and can be applied to a local computer or imported to a Group Policy Object (GPO) in the Active Directory service. When you import a security template to a GPO, Group Policy processes the template and makes the corresponding changes to the members of that GPO, which may be users or computers.
The security Templates snap-in allows you to perform a variety of tasks:

- Customize a predefined security  template
- Define a security template
- Delete a security template
- Refresh the security template list
- Set a description for a security template