

Windows Operating Systems

Basic Security

Objectives

- Explain Windows Operating System (OS) common configurations
- Recognize OS related threats
- Apply major steps in securing the OS

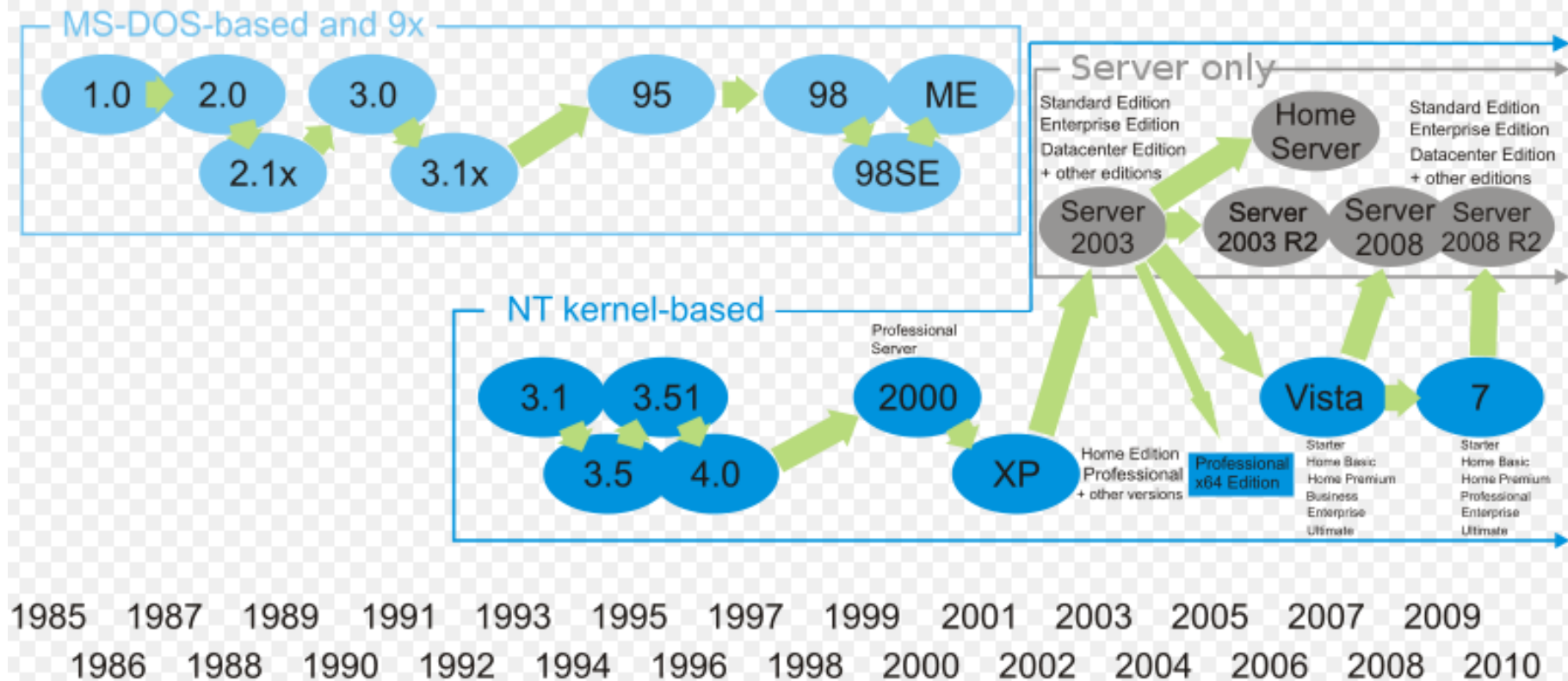
Windows Operating System

- History of Versions
- Control Panel Components
- Local Firewall
- Local Security Policies
- Users and Groups
- Permissions and Rights
- Tools
- Checklist

History of Windows Versions

Microsoft Windows

family tree



http://en.wikipedia.org/wiki/File:Windows_Family_Tree.svg



CyberPatriot

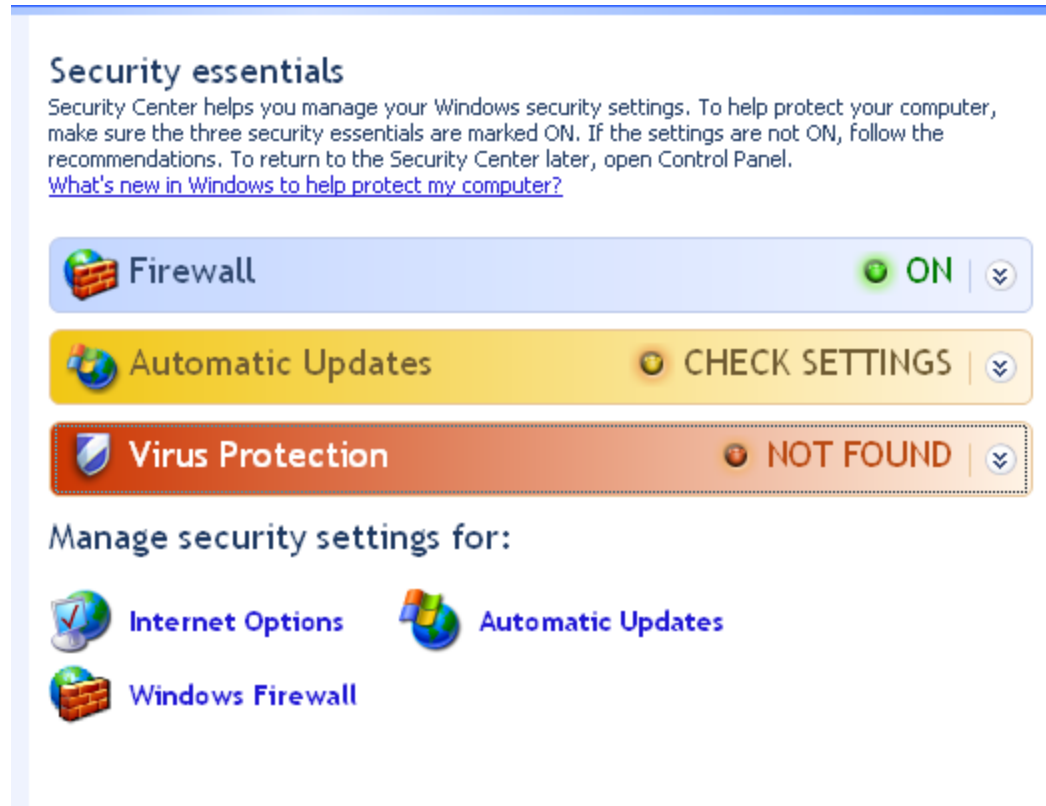
Control Panel

- The control panel is where system changes and configurations can be made for the Windows operating system.
- **Click Start -> Control Panel**



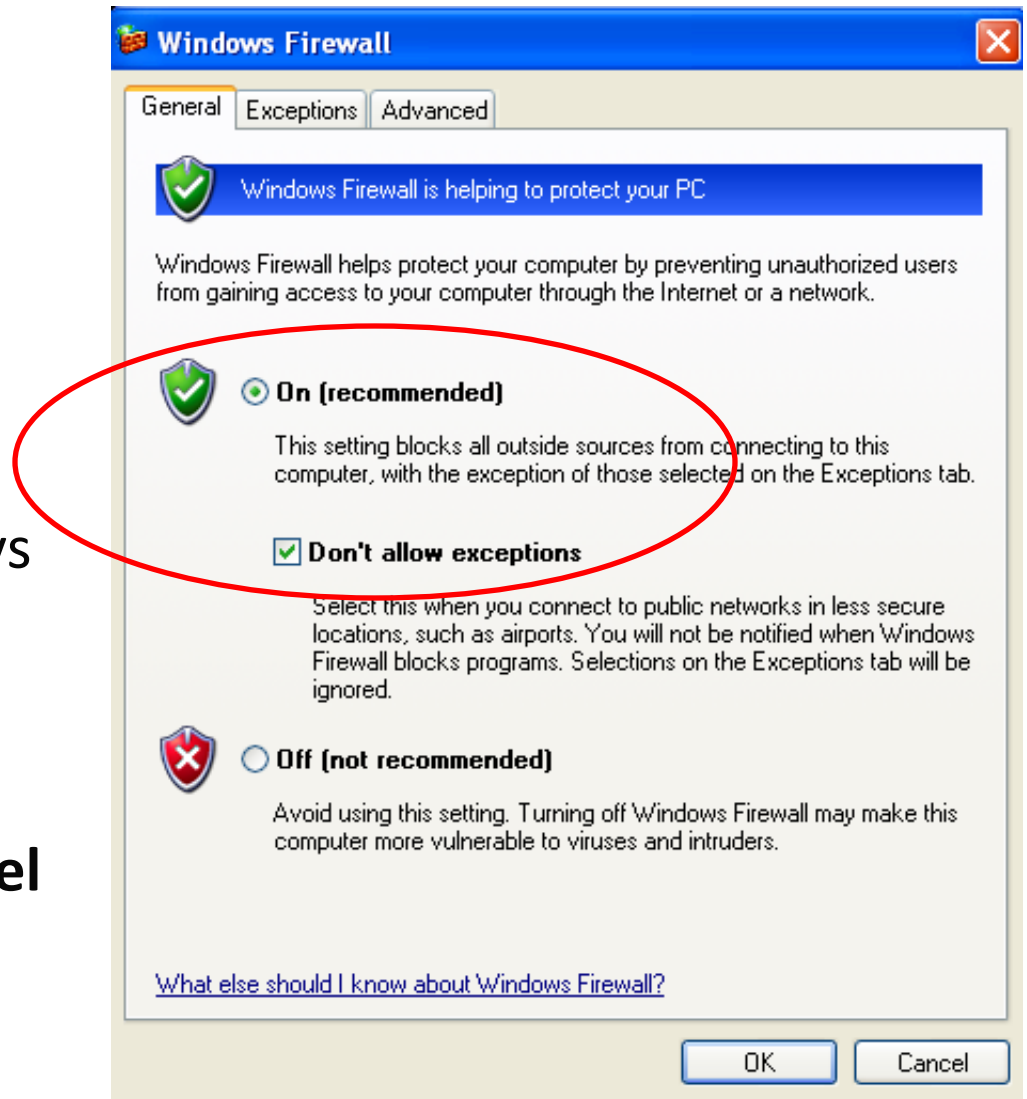
Security Center

- Windows Security Center can help enhance your computer's security by checking the status of several security essentials on your computer, including firewall settings, Windows automatic updating, anti-malware software settings, Internet security settings, and User Account Control settings.
- **Click Start -> Control Panel -> Security Center**



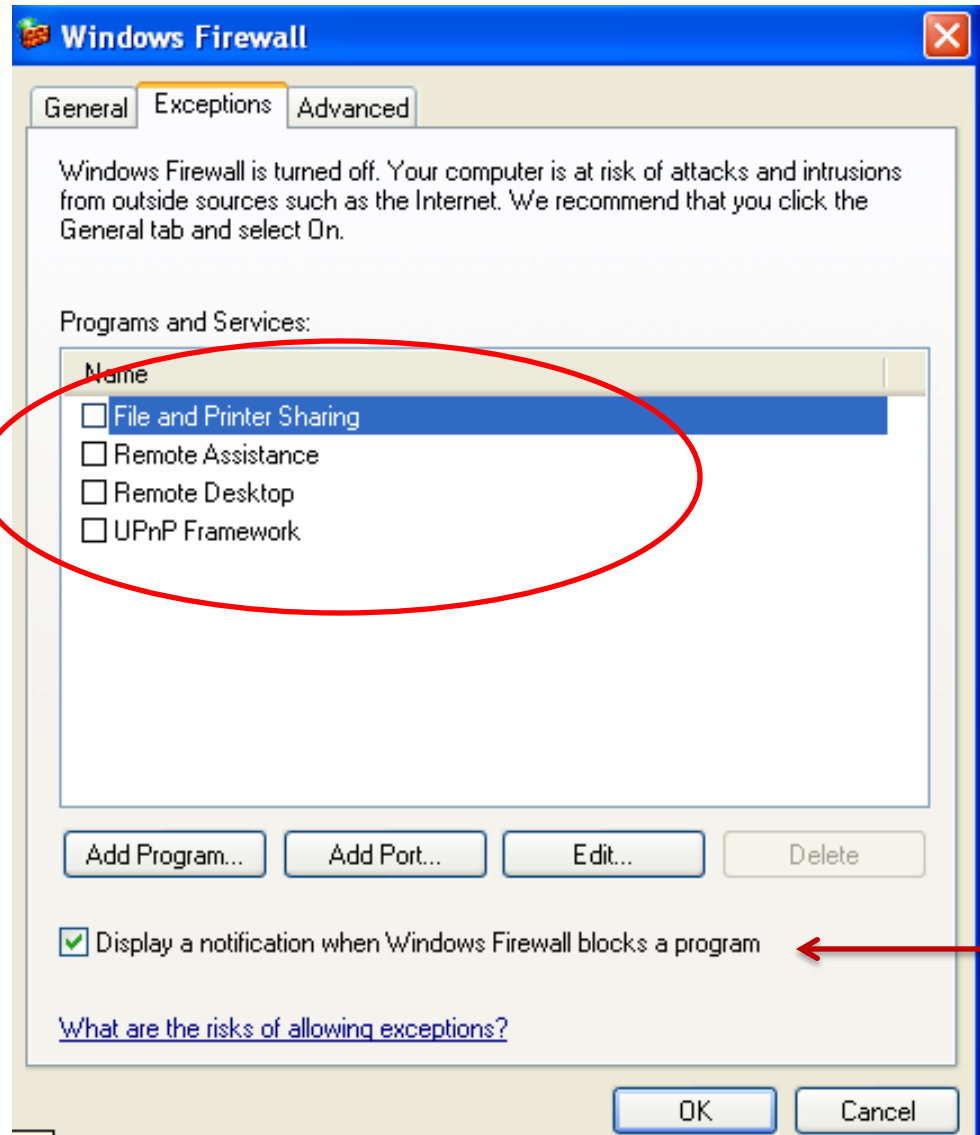
Local Firewall – General Tab

- Firewalls are designed to prevent unauthorized access to a system. They can be implemented via hardware or software.
- A firewall is essential to security and should always be turned 'on'. These settings are under the 'Exceptions' tab
- **Click Start -> Control Panel -> Security Center -> Windows Firewall**



Local Firewall – Exceptions Tab

- The Exceptions tab
 - Allow unsolicited requests to connect to a program on your computer
 - Be more specific about where the request is allowed to initiate from
 - Select **Display a notification when Windows Firewall blocks a program** to be notified



Local Firewall – Exceptions Tab

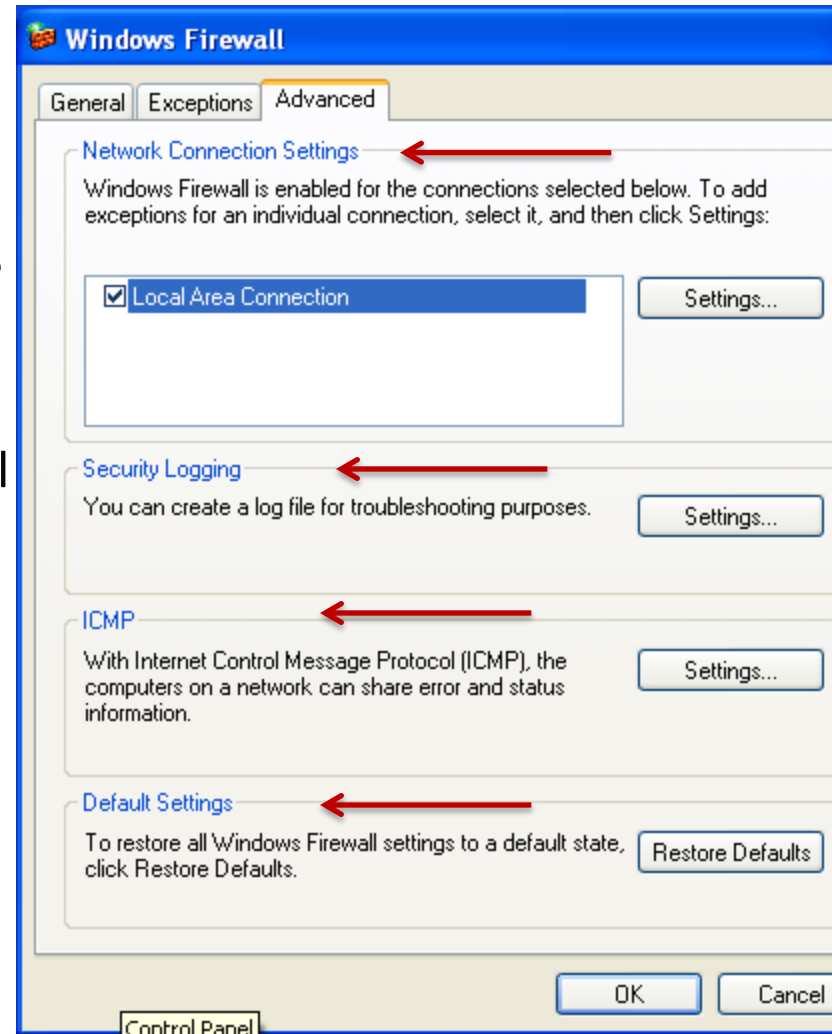
- File and Printer Sharing
 - Allows you to share the contents of selected folders and locally attached printers with other computers
- Remote Assistance
 - Allows a user to temporarily control a remote Windows computer over a network or the Internet to resolve issues
- Remote Desktop
 - Allows older Windows platforms to remotely connect to a computer running Windows XP
- UPnP Framework
 - Allows "plug-and-play" devices to connect to a network and automatically establish working configurations with other devices

Programs and Services:

Name	
<input type="checkbox"/>	File and Printer Sharing
<input type="checkbox"/>	Remote Assistance
<input type="checkbox"/>	Remote Desktop
<input type="checkbox"/>	UPnP Framework

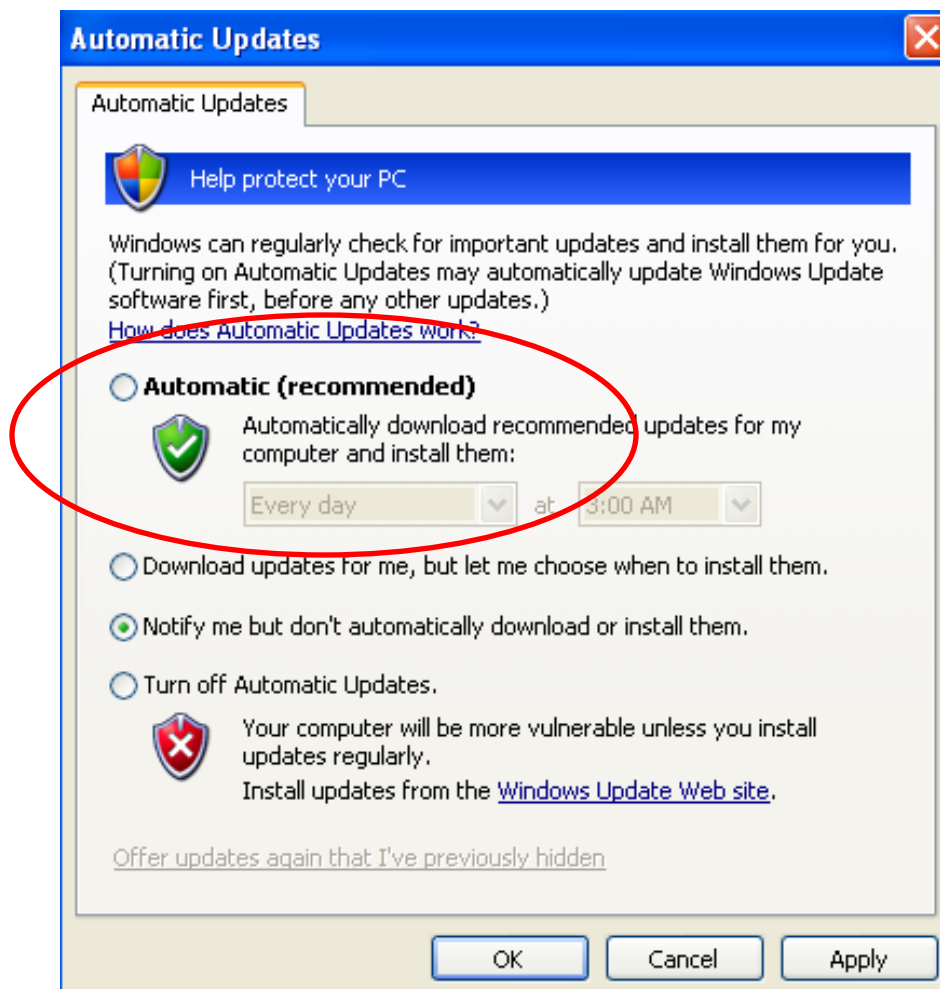
Local Firewall – Advanced Tab

- The Advanced tab
 - Network connection settings - define Windows Firewall settings for individual hardware connections that are available on a computer
 - Security Logging - create a record of successful connections and unsuccessful connection attempts across Windows Firewall
 - ICMP (Internet Control Message Protocol) - select which parts of ICMP can be used through Windows Firewall
 - Default Settings - restore Windows Firewall settings to their original defaults settings.



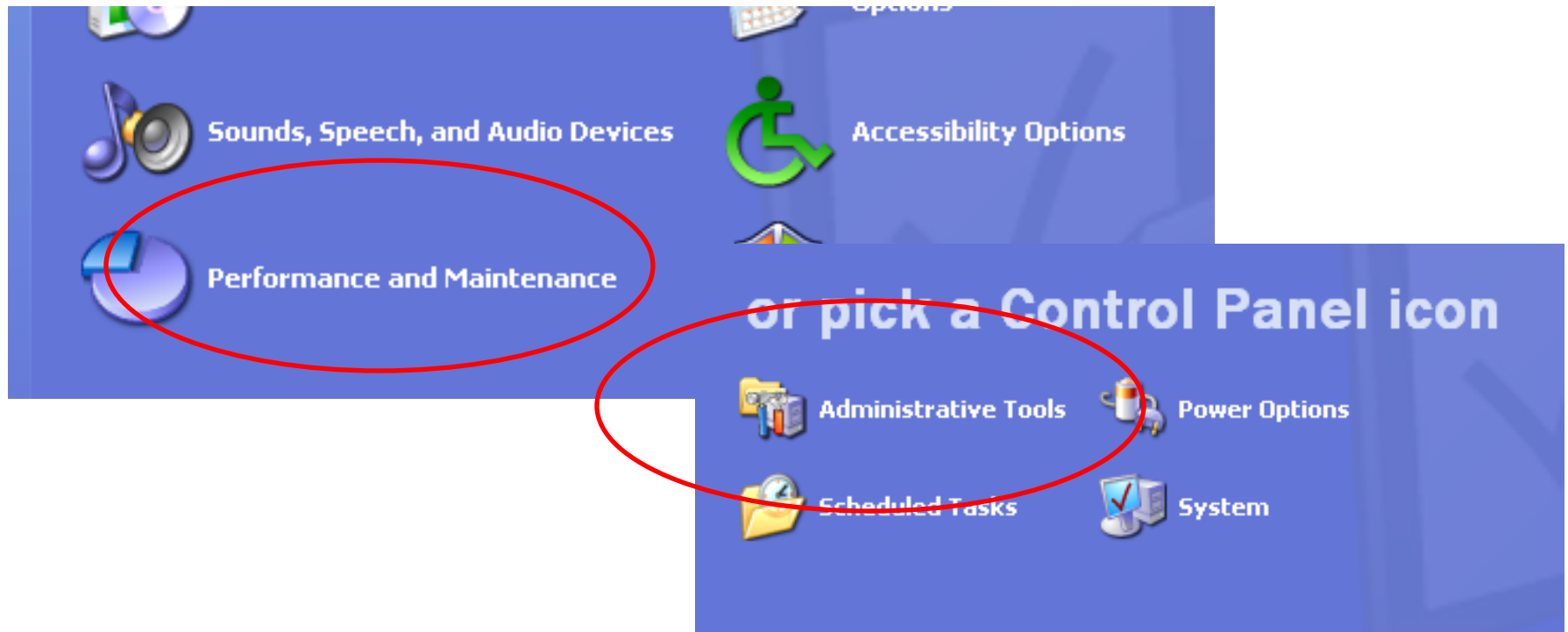
Automatic Updates

- Because updates should be tested before applied, always set 'Automatic' for Automatic Update settings.



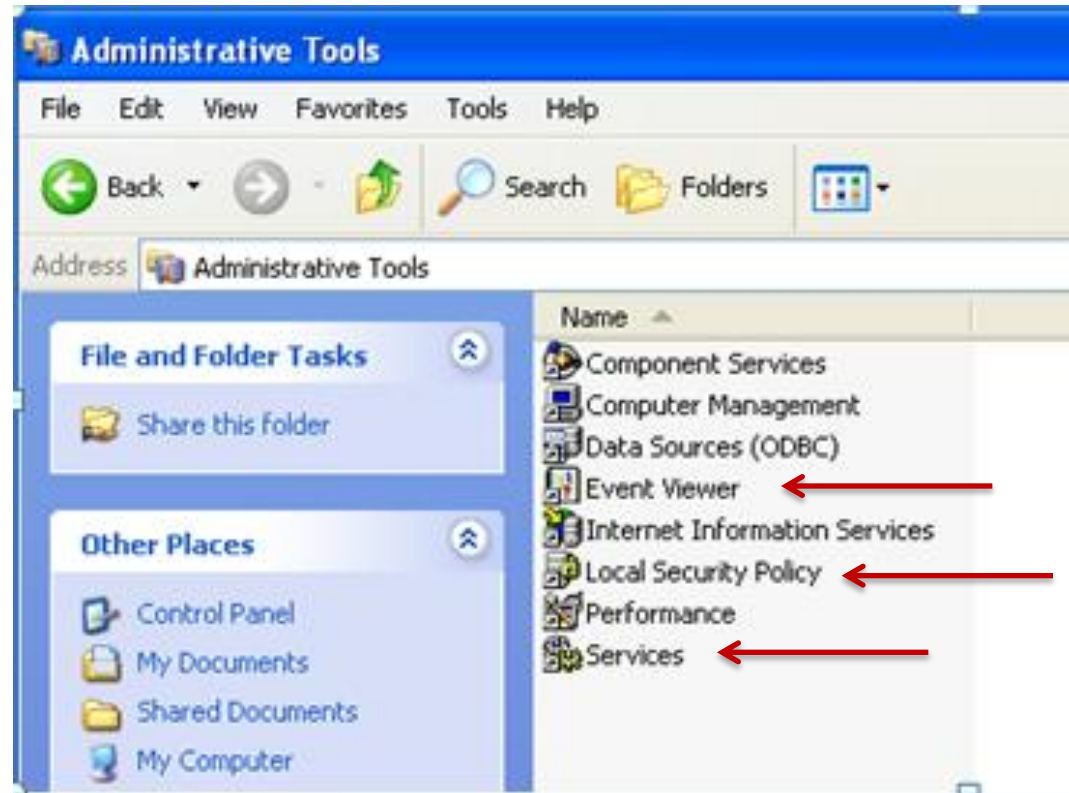
Performance and Maintenance

- Administrative Tools is where you define your policies and monitor system activity.
- Click Start -> Control Panel -> Performance and Maintenance -> Administrative Tools



Administrative Tools

- **Local Security Policy** - view and edit group policy settings
 - Group Policy is a set of rules which control the working environment of user accounts and computer accounts
- **Event Viewer** - records application, security, and system events
- **Services** - lists all available on the system and their status



Local Security Policies

- Local Security Policies enforce standards amongst the organization to strengthen its security posture as a whole
- Click Start -> Control Panel -> Performance and Maintenance -> Administrative Tools -> Local Security Policy
 - Password policy
 - Defining and enforcing strong password policies for an organization can help prevent attackers from impersonating users and help prevent the loss, exposure, or corruption of sensitive information
 - Account lockout policy
 - Disables a user account if an incorrect password is entered a specified number of times over a specified period
 - Audit policies
 - Monitoring the creation or modification of objects gives a way to track potential security problems, helps to ensure user accountability, and provides evidence in the event of a security breach



Local Security Policies

- Define a strong password policy
 - **Enforce password history** – set to “5”. A user cannot use the same password when their password expires.
 - **Maximum password age** - default is "42". This specifies how long a user can use the same password. After 42 days, the user must change his/her password. Set to “90” for user accounts and “30” for administrator.
 - **Minimum password length** - set to "8". This means that a password must be at least 8 characters long.
 - **Password must meet complexity requirements** - set to "Enabled". This means a password must include upper and lower case letters, a number and a special character.
 - **Store password using reversible encryption for all users in the domain** - always leave "Disabled". If you enable this policy, all users' passwords will be easy to crack.



Local Security Policies

- Define an account lockout policy
 - These policy settings help you to prevent attackers from guessing users' passwords, and they decrease the likelihood of successful attacks on your network.
 - **Account lockout duration** - the number of minutes a locked-out account remains locked out before automatically becoming unlocked
 - **Account lockout threshold** - the number of failed logon attempts that causes a user account to be locked out
 - **Reset account lockout counter after** - the number of minutes that must elapse before the failed logon attempt counter is reset to 0
 - Be careful not to set these too low. If users lock themselves out because of mistyping their passwords, this can provide for more work for your organization.

Local Security Policies

- Define audit policies
 - Audit policies must be set and enabled for logs to be available in the Event Viewer
 - **Audit account logon events** – enable to prevent random hacks or stolen passwords
 - **Audit object access** – enable to prevent improper access to sensitive files
 - **Audit process tracking** – enable to monitor attempts to modify program files to help detect virus outbreaks
 - **Account management** - enable to see if a change has occurred to an account name, enabled or disabled an account, created or deleted an account, changed a password, or changed a user group










Local Security Policies

- **Directory service access** – enable to track accesses to an Active Directory® directory service object that has its own system access control list (SACL)
- **Logon events** – enable to see when someone has logged on or off to the computer
- **Privilege use** – enable to see when someone performs a user right
- **Policy change** - enable to see attempts to change local security policies, user rights assignments, auditing policies, or trust policies
- **System events** - enable to see when someone has shut down or restarted the computer, or when a process or program tries to do something it does not have permission to do

Local Security Policies

- **Security Setting**

- **Success** setting generates an event when the requested action succeeds
- **Failure** setting generates an event when the requested action fails
- **No Auditing** does not generate an event for the associated action

Policy	Security Setting
 Audit account logon events	Success, Failure
 Audit account management	Success, Failure
 Audit directory service access	No auditing
 Audit logon events	Success, Failure
 Audit object access	No auditing
 Audit policy change	Success, Failure
 Audit privilege use	Failure
 Audit process tracking	Failure
 Audit system events	Failure

Local Security Policies

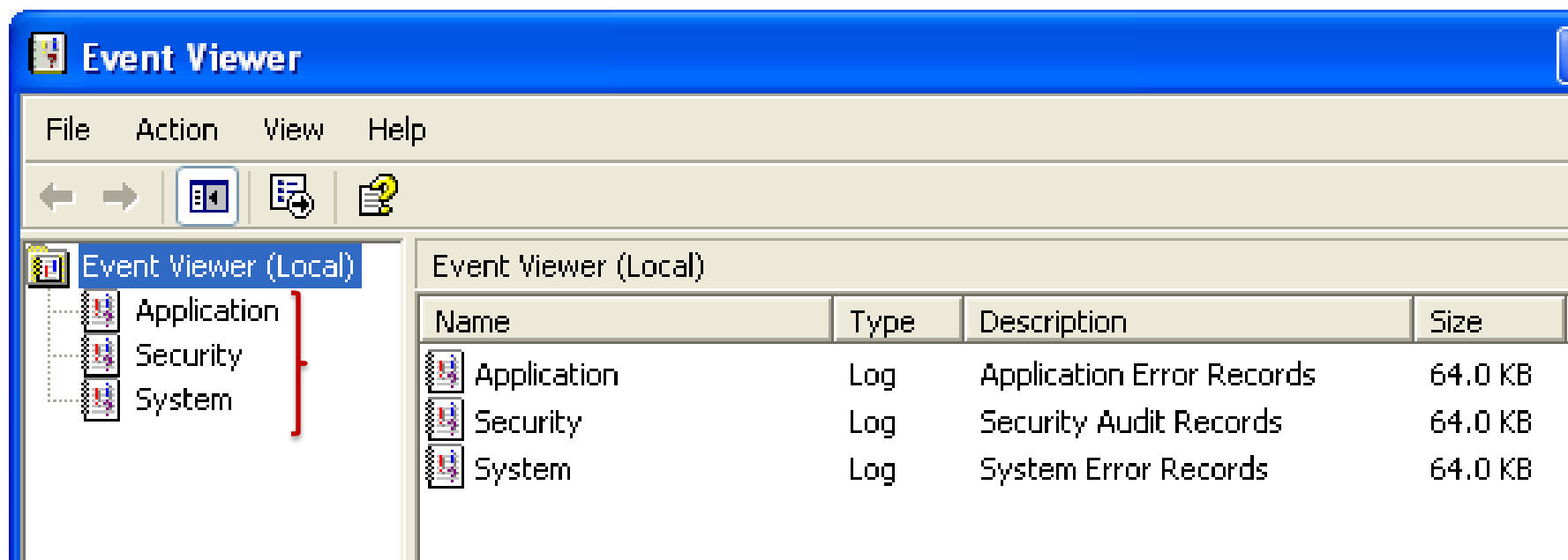
- Windows XP grants the "Everyone" account the ability to access your computer over the network
- Remove "Everyone" Access to Your Computer
 - By deleting the Everyone account, you gain more control over who can access your XP system
- To remove access to your computer by the Everyone account
 - Click Start-> Control Panel ->Performance and Maintenance -> Administrative Tools -> Local Security Policy
 - In the Security Settings tree, click Local Policies ->User Rights Assignment
 - In the right pane, double click the setting for Access this computer from the Network

Event Viewer

- Event Viewer
 - Click Start -> Control Panel -> Performance and Maintenance -> Administrative Tools -> Event Viewer
- Displays logs that capture events occurring on the system
- These logs are based on the policies you have created and/or enabled (local security policy, audit policies, etc.)
- Logs sources for use by the Windows operating system and Windows applications respectively
- Three log sources: System, Application and Security

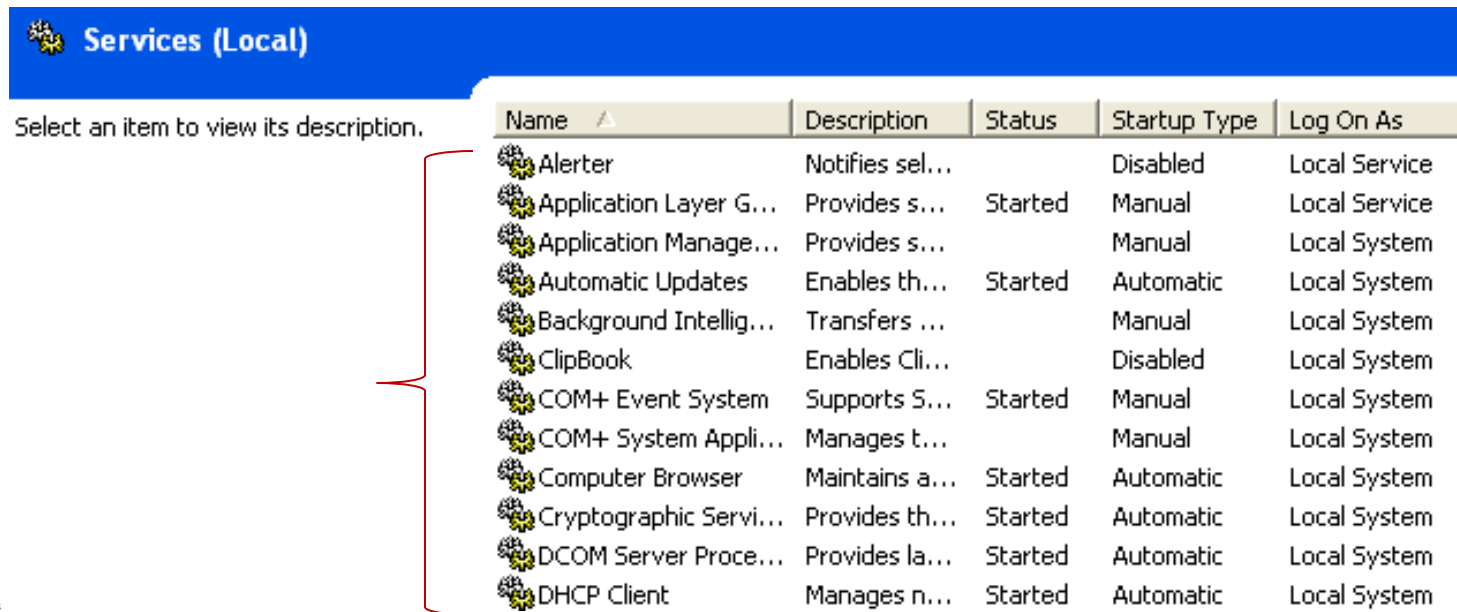
Event Viewer

- Application log – events logged by programs
- Security log - any successful or unsuccessful logon attempts
- System log - events logged by system components (i.e., driver fails to load during startup)



Services










- Services are programs that run invisibly in the background on a system (e.g., RemoteAccess, DHCP, Spooler, etc.)
- They load and run whether or not anyone logs into the system
- To view all available services
 - Click Start -> Control Panel -> Performance and Maintenance -> Administrative Tools -> Services



Name	Description	Status	Startup Type	Log On As
Alerter	Notifies sel...		Disabled	Local Service
Application Layer G...	Provides s...	Started	Manual	Local Service
Application Manage...	Provides s...		Manual	Local System
Automatic Updates	Enables th...	Started	Automatic	Local System
Background Intellig...	Transfers ...		Manual	Local System
ClipBook	Enables Cli...		Disabled	Local System
COM+ Event System	Supports S...	Started	Manual	Local System
COM+ System Appli...	Manages t...		Manual	Local System
Computer Browser	Maintains a...	Started	Automatic	Local System
Cryptographic Servi...	Provides th...	Started	Automatic	Local System
DCOM Server Proce...	Provides la...	Started	Automatic	Local System
DHCP Client	Manages n...	Started	Automatic	Local System

Services

- Services are configured by Startup Type
 - Automatic - service starts automatically when the system starts or when the service is called for the first time
 - Manual – service must be started manually before it can be loaded by the operating system and made available for use
 - Disabled - cannot be started automatically or manually

Name ▲	Description	Status	Startup Type	Log On As
 Alerter	Notifies sel...		Disabled	Local Service
 Application Layer G...	Provides s...	Started	Manual	Local Service
 Application Manage...	Provides s...		Manual	Local System
 Automatic Updates	Enables th...	Started	Automatic	Local System
 Background Intellig...	Transfers ...		Manual	Local System
 ClipBook	Enables Cli...		Disabled	Local System
 COM+ Event System	Supports S...	Started	Manual	Local System
 COM+ System Appli...	Manages t...		Manual	Local System
 Computer Browser	Maintains a...	Started	Automatic	Local System

Services

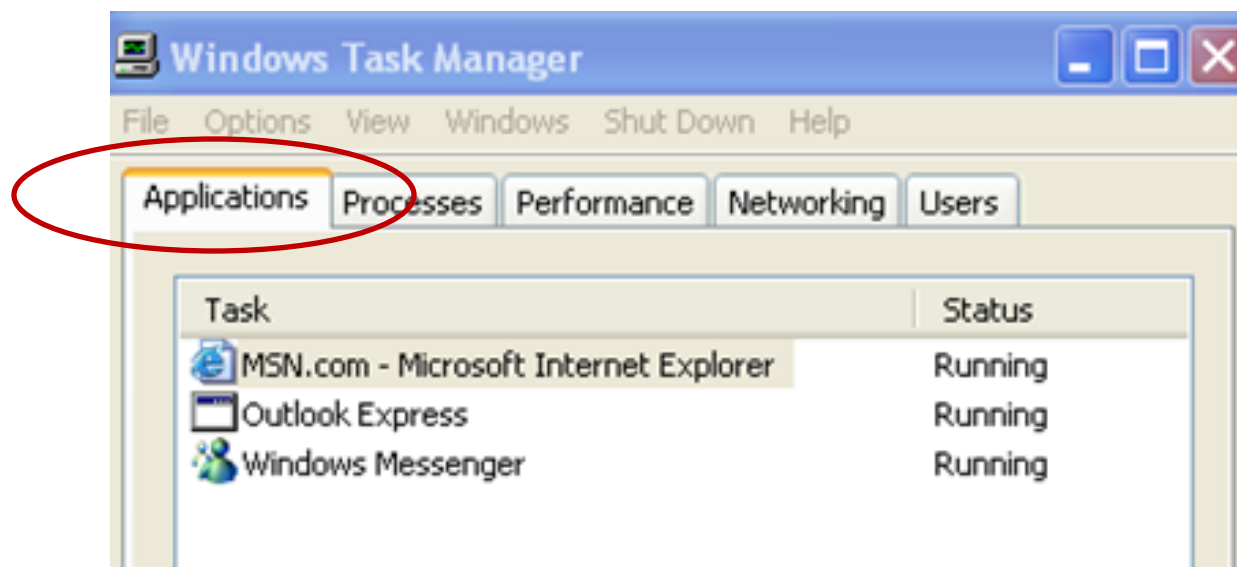
- Disable unnecessary services
 - Turning off unnecessary services can greatly reduce your exploit risk, while improving system performance
 - IIS – web server capabilities
 - NetMeeting Remote Desktop Sharing - VoIP
 - Remote Desktop Help Session Manager
 - Remote Registry – allows remote users to edit registry
 - Routing and Remote Access - allows the system to be used as a router
 - Simple File Sharing
 - SSDP Discovery Service – plug and play
 - Telnet – allows remote users to log on
 - Universal Plug and Play Device Host – installation of plug and play devices
 - Windows Messenger Service – not necessary to use windows instant messenger; allows 'net send' command to be used

Performance Monitoring

- Performance monitoring
 - Viewing performance data for the system, both in real time and from log files
 - Obtain information about hardware, software, and system components, and monitor security events on a local or remote computer
 - Allows you to see what processes may be over utilizing resources or not functioning properly
 - Monitor processes to see if unknown programs are running
 - Identify and diagnose the source of current system problems, or help you predict potential system problems

Performance Monitoring

- Task Manager will show programs, services, and processes currently running on the system
- The Applications Tab
 - Allows you to see all programs currently running
 - Allows you to select a program and terminate it
- Right Click on the Menu Bar -> Click Task Manager -> Applications Tab to see applications and their current status

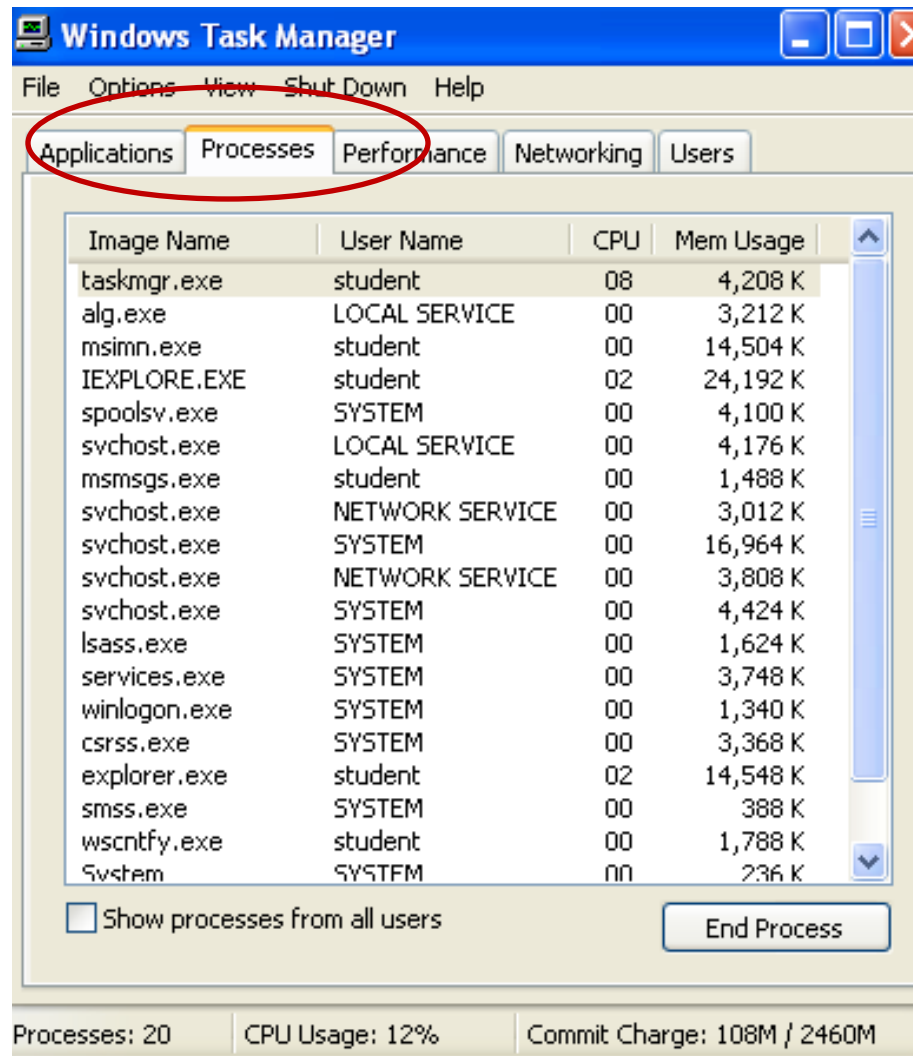


Performance Monitoring

- Task Manager functions
 - Show programs, services, and processes currently running on the system
 - Show network activity and resource utilization
 - Terminate processes, etc.
 - Set process priorities
 - A common target for malware
 - Some malware processes (rootkits) will prevent themselves from being list in the task manager making them harder to detect
- Right Click on the Menu Bar -> Click Task Manager

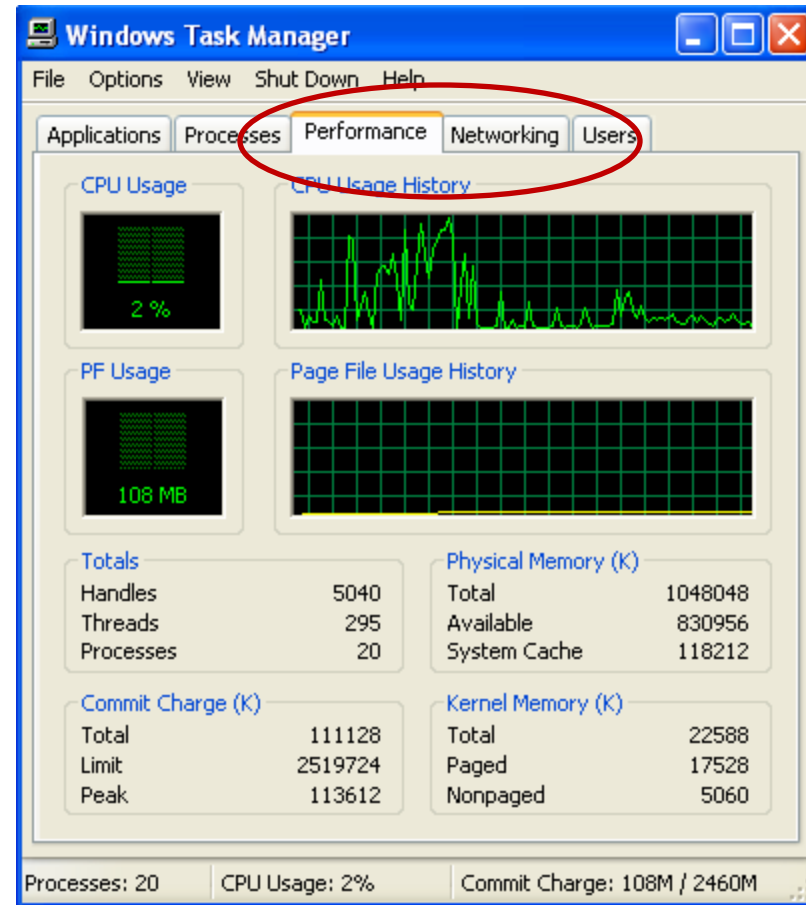
Performance Monitoring

- The Processes Tab
 - Shows all processes running; also shows the owner, CPU usage and Memory Usage of each process
 - Allows you to sort processes based on name, user, cpu or memory usage
- Right Click on the Menu Bar -> Click Task Manager -> Processes Tab



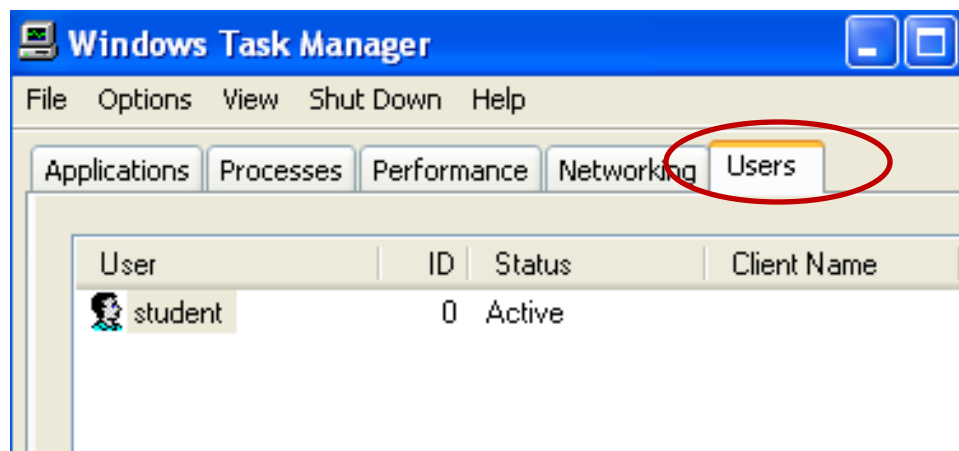
Performance Monitoring

- The Performance tab
 - Monitor performance and resources
 - Overall statistics for system usage
 - CPU usage
 - Memory usage
- Right Click on the Menu Bar -> Click Task Manager -> Performance Tab
- The Networking tab
 - Shows wired and wireless activity in a chart format (network adapter activity)
- Right Click on the Menu Bar -> Click Task Manager -> Networking Tab



Performance Monitoring

- The Users tab
 - Shows all users currently logged into the system
 - Users can be disconnected and/or logged off via this tab
- Right Click on the Menu Bar -> Click Task Manager -> Users Tab

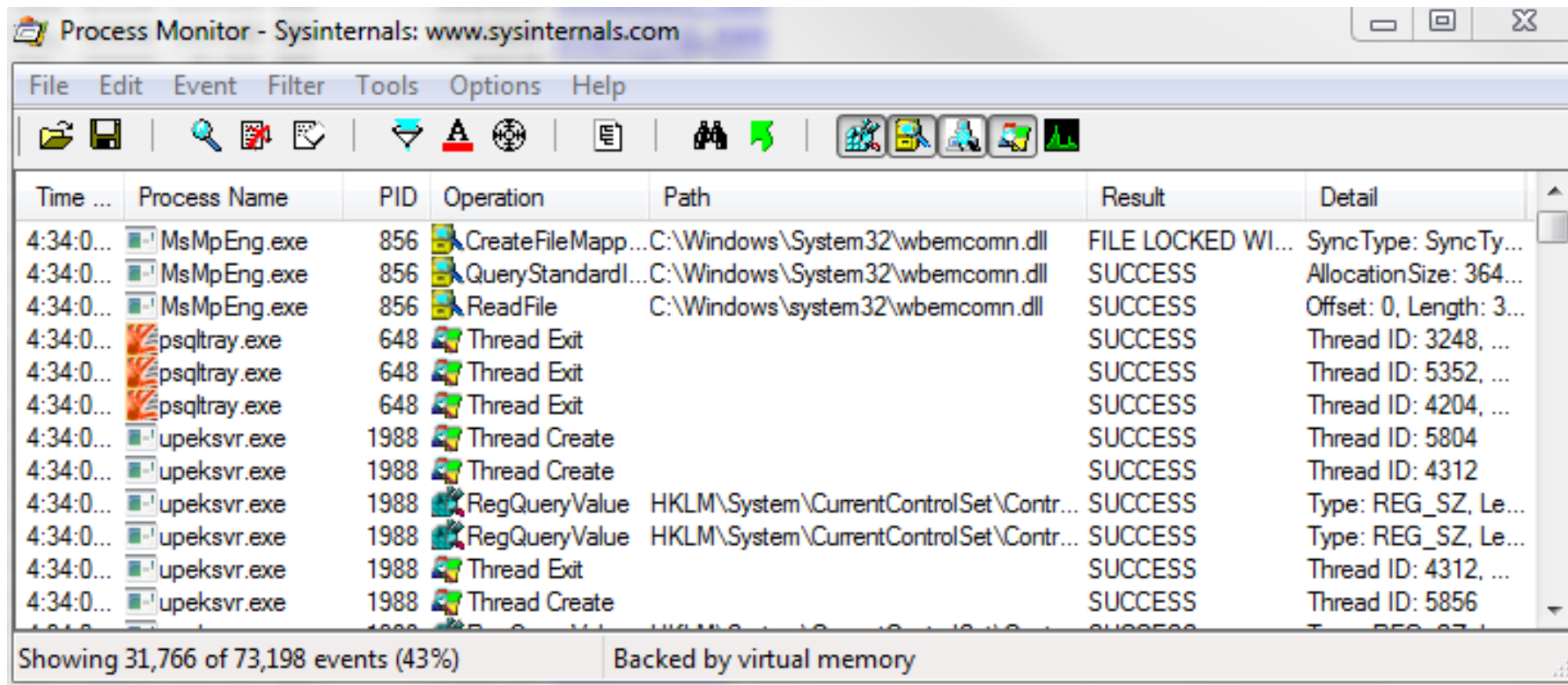


Performance Monitoring

- Sysinternals
 - A third-party tool that helps manage, troubleshoot and diagnose Windows systems and applications
 - <http://technet.microsoft.com/en-us/sysinternals>
 - Tools can be run live from the Internet
 - <http://live.sysinternals.com>
 - File and disk utilities
 - Networking utilities
 - Process utilities
 - Security utilities
 - System information utilities

Performance Monitoring

- Example – Process Monitor utility
 - Monitors real-time file system, Windows registry, processes, threads and DLL activity
 - Name, what the process is doing (operation), the result and details



The screenshot shows the Process Monitor utility window from Sysinternals. The title bar reads "Process Monitor - Sysinternals: www.sysinternals.com". The menu bar includes File, Edit, Event, Filter, Tools, Options, and Help. The toolbar contains icons for file operations, search, filters, and monitoring. The main table displays a list of events with columns for Time, Process Name, PID, Operation, Path, Result, and Detail. The status bar at the bottom indicates "Showing 31,766 of 73,198 events (43%)" and "Backed by virtual memory".

Time ...	Process Name	PID	Operation	Path	Result	Detail
4:34:0...	MsMpEng.exe	856	CreateFileMapp...	C:\Windows\System32\wbemcomn.dll	FILE LOCKED WI...	Sync Type: SyncTy...
4:34:0...	MsMpEng.exe	856	QueryStandardI...	C:\Windows\System32\wbemcomn.dll	SUCCESS	AllocationSize: 364...
4:34:0...	MsMpEng.exe	856	ReadFile	C:\Windows\system32\wbemcomn.dll	SUCCESS	Offset: 0, Length: 3...
4:34:0...	psqltray.exe	648	Thread Exit		SUCCESS	Thread ID: 3248, ...
4:34:0...	psqltray.exe	648	Thread Exit		SUCCESS	Thread ID: 5352, ...
4:34:0...	psqltray.exe	648	Thread Exit		SUCCESS	Thread ID: 4204, ...
4:34:0...	upeksvr.exe	1988	Thread Create		SUCCESS	Thread ID: 5804
4:34:0...	upeksvr.exe	1988	Thread Create		SUCCESS	Thread ID: 4312
4:34:0...	upeksvr.exe	1988	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Le...
4:34:0...	upeksvr.exe	1988	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Le...
4:34:0...	upeksvr.exe	1988	Thread Exit		SUCCESS	Thread ID: 4312, ...
4:34:0...	upeksvr.exe	1988	Thread Create		SUCCESS	Thread ID: 5856



User Accounts

- Local Users and Groups limit the ability of users and groups to perform certain actions by assigning them rights and permissions
- User accounts
 - A collection of information that tells Windows what files a user can access, what changes a user can make
 - Allow multiple users to share a computer, but still have their own files and settings
 - Each user accesses their user account with a user name and password
- Administrator account
 - Can change security settings, install software and hardware, and access all files on the computer; including make changes to other user accounts

User and Group Account Permissions

- Permissions are customizable by individual user or by a group of users
 - **Full Control** – all file permissions granted (administrator level)
 - **Modify** – permission to change content but not ownership of files; cannot delete files or folders
 - **Read & Execute** - permission allows or denies the user to read and execute files
 - **List Folder Contents** - permission allows or denies the user from viewing file names
 - **Read** - permission allows or denies the user from viewing the attributes of a file or folder
 - **Write** - permission applies only to files and allows or denies the user from making changes to the file and overwriting existing content by NTFS

User and Group Account Permissions

- Inherited permissions
 - If an object's permissions are shaded, the object has inherited permissions from the parent object
- Three ways to make changes to inherited permissions
 - Make the changes to the parent object, and then the object will inherit these permissions
 - Select the opposite permission (**Allow** or **Deny**) to override the inherited permission
 - Clear the **Inherit from parent the permission entries that apply to child objects**

Account Permissions Best Practices

- User accounts settings
 - Limit Administrative Privileges
 - Make sure user accounts are set to 'limited'
 - Do not give 'full control' as that equals Administrator access
 - Running as Administrator may allow malicious software to gain access
 - Make sure all accounts have passwords
 - Disable Guest account
- Administrator account
 - Change password - Administrator account has default or no password upon initial installation
 - Obfuscate the account - change name
 - Don't use the account
 - Websites have default passwords published
 - <http://www.phenoelit-us.org/dpl/dpl.html>

Local vs. Domain Accounts

- Local account
 - Username and encrypted password are stored on the computer itself
 - Permissions apply only to this computer
- Domain account
 - Resides on a *Domain Controller*
 - A server that manages access to a set of network resources such as print servers, applications, etc.
 - A user can log into the domain controller and is given permissions to all network resources
 - Username and password are stored on a domain controller rather than on each computer the user accesses
 - Permissions apply to a network of computers and peripherals
 - Network administrators only have one place to store user information

Tools

- Microsoft Baseline Security Analyzer (MBSA)
 - Free vulnerability assessment tool for the Microsoft platform
 - Helps with the assessment phase of an overall security management strategy for legacy platforms and products
 - Can perform local or remote scans of Windows systems
 - Checks for
 - Insecure security settings
 - Windows administrative vulnerabilities
 - Weak passwords
 - IIS and SQL administrative vulnerabilities
 - To download the latest version go to
 - <http://technet.microsoft.com/en-us/security/cc184923>

Tools

- Microsoft Update

- Creates an inventory of applicable and installed security updates and service packs on each computer
- Configures the hierarchy for weekly scanning of all computers to identify security update compliance levels
- Integrates software update management features of Windows and Microsoft Update with the existing SMS 2003 Software update management feature. This means you can now take advantage of a single tool for Windows, Office, SQL Server, Exchange updates, etc.
- Automated task obtains the latest catalog of updates
- Creates reports to help monitor software update compliance and distribution status
- Located in the Control Panel or
 - Click Start -> All programs -> Windows Update

First Steps to Securing a Machine

- Install the operating system and components (such as hardware drivers, system services, and so on).
- Install Service Packs and Windows Updates.
- Update installed applications (Adobe Reader, Flash, etc).
- Install anti-virus/anti-spyware utilities and scan for malware
- Configure critical operating system parameters (such as password policy, access control, audit policy, kernel mode driver configuration, and so on).
- Take ownership of files that have become inaccessible.
- Configure and monitor the security and auditing logs.
- When it is clean and secure, back up the system and create a restore point.



Checklist

- Disable unnecessary services
- Disable dangerous features
- Employ email security practices
- Install and maintain malware protection software
- Patch more than just the OS
- Research and test updates
- Use a desktop firewall
- Look for alternatives to default applications

List of References

- <http://technet.microsoft.com/>
- http://www.sans.org/score/checklists/ID_Windows.pdf
- http://en.wikipedia.org/wiki/File:Windows_Family_Tree.svg
- <http://technet.microsoft.com/en-us/library/cc875811.aspx>
- <http://help.artaro.eu/index.php/windows-xp/essential-administration-xp/local-security-policy-xp.html>
- <http://www.phenoelit-us.org/dpl/dpl.html>
- <http://www.techrepublic.com/blog/security/10-services-to-turn-off-in-ms-windows-xp/354>