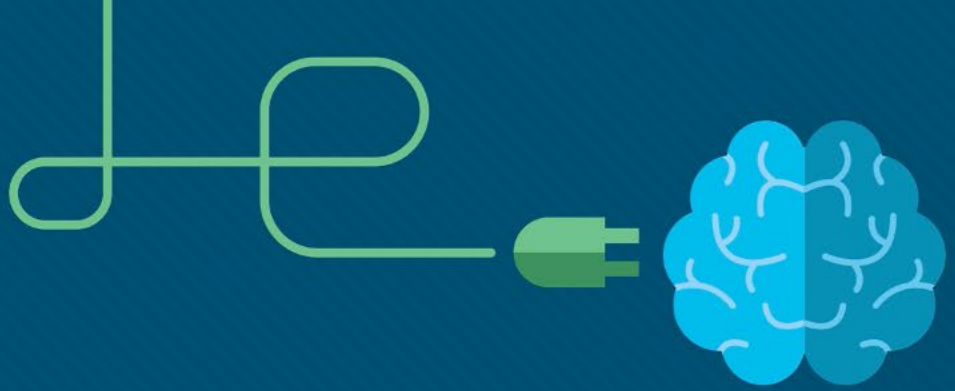


Module 7: The Windows Operating System

Cybersecurity Essentials 3.0

Module Objectives

Module Title: The Windows Operating System
Module Objective: Use Windows administrative tools.

Topic Title	Topic Objective
Windows History	Describe the history of the Windows Operating System.
Windows Architecture and Operations	Explain the architecture of Windows and its operation.
Windows Configuration and Monitoring	Use Windows administrative tools to configure, monitor, and manage system resources.
Windows Security	Explain how Windows can be kept secure.

7.1 Windows History

Disk Operating System

```
Starting MS-DOS...
HIMEM is testing extended memory... done.
C:\> C:\DOS\SMARTDRV.EXE /X
C:\> dir
Volume in drive C is MS-DOS_6
Volume Serial Number is 4006-6939
Directory of C:\
DOS         <DIR>         05-06-17  1:09p
COMMAND  COM       54,645 05-31-94  6:22a
WINA20   386        9,349 05-31-94  6:22a
CONFIG   SYS           71 05-06-17  1:10p
AUTOEXEC BAT           78 05-06-17  1:10p
        5 file(s)         64,143 bytes
                  517,021,696 bytes free
C:\>
```

The first computers did not have modern storage devices such as hard drives, optical drives, or flash storage. The first storage methods used punch cards, paper tape, magnetic tape, and even audio cassettes.

Floppy disk and hard disk storage require software to read from, write to, and manage the data that they store. The Disk Operating System (DOS) is an operating system that the computer uses to enable these data storage devices to read and write files.

Disk Operating System (Cont.)

- Microsoft bought DOS and developed MS-DOS.
- With MS-DOS, the computer had a basic working knowledge of how to access the disk drive and load the operating system files directly from disk as part of the boot process.
- Early versions of Windows consisted of a Graphical User Interface (GUI) that ran over MS-DOS.
- To experience a little of what it was like to work in MS-DOS, open a command window by typing **cmd** in Windows Search and pressing **Enter**.
  - The table lists some commands that you can use.
  - Enter **help** followed by the command to learn more about the command.

Disk Operating System (Cont.)

MS-DOS Command	Description
dir	Shows a listing of all the files in the current directory (folder)
cd *directory*	Changes the directory to the indicated directory
cd ..	Changes the directory to the directory above the current directory
cd \	Changes the directory to the root directory (often C:)
copy *source destination*	Copies files to another location
del *filename*	Deletes one or more files
find	Searches for text in files
mkdir *directory*	Creates a new directory
ren *oldname newname*	Renames a file
help	Displays all the commands that can be used, with a brief description
help *command*	Displays extensive help for the indicated command

Windows Versions

- Since 1993, there have been more than 20 releases of Windows that are based on the NT operating system.
  - Most of these versions were for use by the public and businesses because of the file security offered by the file system that was used by the NT OS.

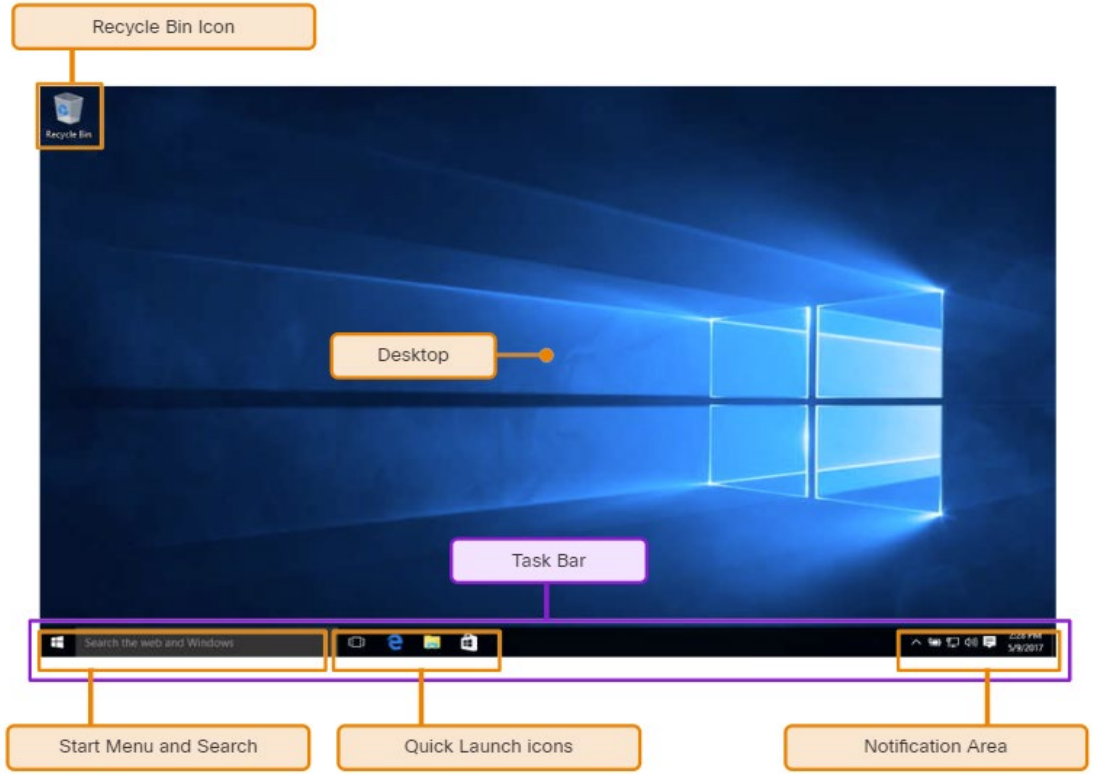
- Beginning with Windows XP, a 64-bit edition was available.
- It had a 64-bit address space instead of a 32-bit address space.
  - In general, 64-bit computers and operating systems are backward-compatible with older 32-bit programs, but 64-bit programs cannot be run on older 32-bit hardware.

- With each subsequent release of Windows, the operating system has become more refined by incorporating more features.
  - Windows 7 was offered with six different editions, Windows 8 with as many as five, and Windows 10 with eight different editions!

Windows Versions (Cont.)

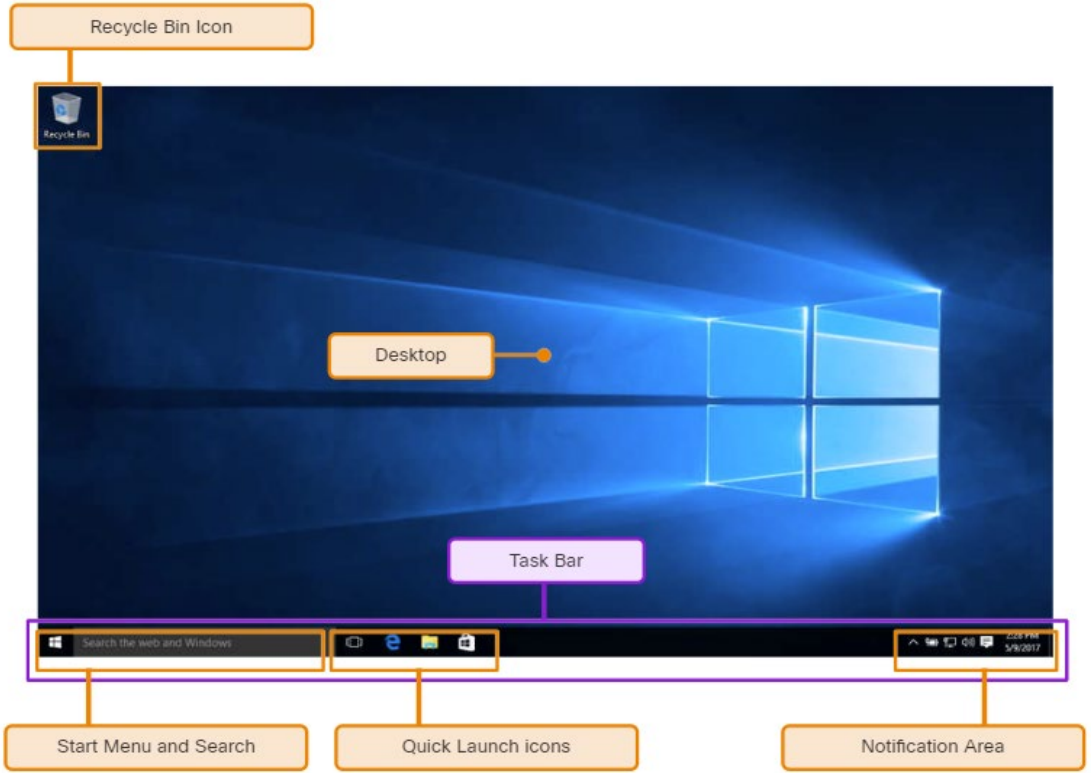
OS	Versions
Windows 7	Starter, Home Basic, Home Premium, Professional, Enterprise, Ultimate
Windows Server 2008 R2	Foundation, Standard, Enterprise, Datacenter, Web Server, HPC Server, Itanium-Based Systems
Windows Home Server 2011	None
Windows 8	Windows 8, Windows 8 Pro, Windows 8 Enterprise, Windows RT
Windows Server 2012	Foundation, Essentials, Standard, Datacenter
Windows 8.1	Windows 8.1, Windows 8.1 Pro, Windows 8.1 Enterprise, Windows RT 8.1
Windows Server 2012 R2	Foundation, Essentials, Standard, Datacenter
Windows 10	Home, Pro, Pro Education, Enterprise, Education, IoT Core, Mobile, Mobile Enterprise
Windows Server 2016	Essentials, Standard, Datacenter, Multipoint Premium Server, Storage Server, Hyper-V Server

Windows GUI



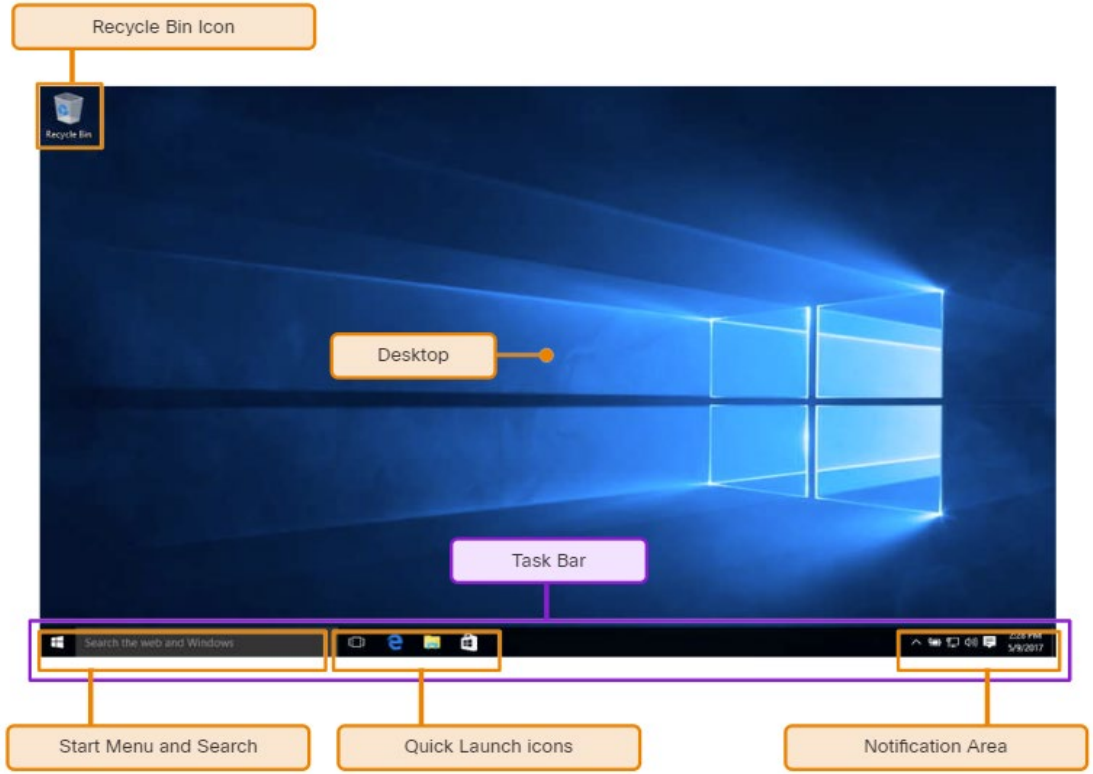
Windows has a graphical user interface (GUI) for users to work with data files and software. The GUI has a main area that is known as the Desktop, shown in the figure.

Windows GUI (Cont.)



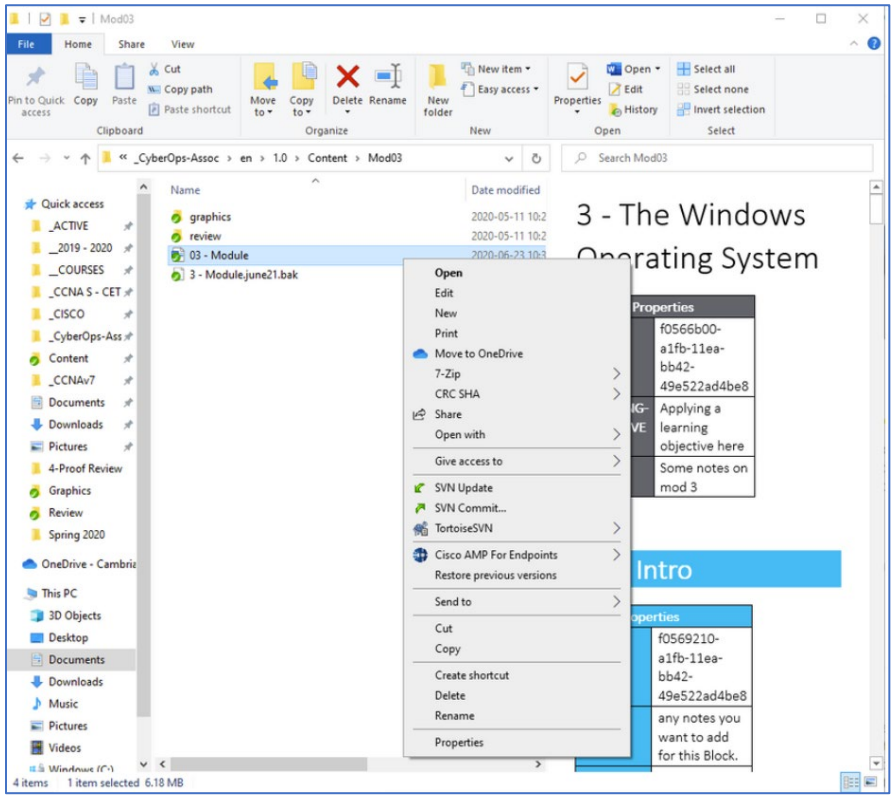
- The Desktop can be customized with various colors and background images.
- Windows supports multiple users, so each user can customize the Desktop to their liking.
- The Desktop can store files, folders, shortcuts to locations and programs, and applications.
- The Desktop also has a recycle bin icon, where files are stored when the user deletes them.
- Files can be restored from the recycle bin or the recycle bin can be emptied of files, which truly deletes them.

Windows GUI (Cont.)



- The Task Bar has three areas that are used for different purposes.
- Start menu - used to access all the installed programs, configuration options, and the search feature.
- Task Bar - users place quick launch icons that run specific programs or open specific folders when they are clicked.
- Notification area – shows the functionality of many different programs and features.

Windows GUI (Cont.)



Right-clicking an icon will bring up additional functions that can be used.

This list is known as a Context Menu, shown in the figure.

There are Context Menus for the icons in the notification area, for quick launch icons, system configuration icons, and for files and folders.

Operating System Vulnerabilities

- Operating systems consist of millions of lines of code. Installed software can also contain millions of lines of code. With all this code comes vulnerabilities.
- A vulnerability is some flaw or weakness that can be exploited by an attacker to reduce the viability of a computer's information.
- To take advantage of an operating system vulnerability, the attacker must use a technique or a tool to exploit the vulnerability.
- The attacker can then use the vulnerability to get the computer to act in a fashion outside of its intended design.
- In general, the goal is to gain unauthorized control of the computer, change permissions, or to manipulate or steal data.

Operating System Vulnerabilities (Cont.)

Some common Windows OS security recommendations include:

Recommendation	Description
Virus or malware protection	• By default, Windows uses Windows Defender for malware protection. • Windows Defender provides a suite of protection tools built into the system. • If Windows Defender is turned off, the system becomes more vulnerable to attacks and malware.
Unknown or unmanaged services	• There are many services that run behind the scenes. • It is important to make sure that each service is identifiable and safe. • With an unknown service running in the background, the computer can be vulnerable to attack.
Encryption	• When data is not encrypted, it can easily be gathered and exploited. • This is not only important for desktop computers, but especially mobile devices.
Security policy	• A good security policy must be configured and followed. • Many settings in the Windows Security Policy control can prevent attacks.

Operating System Vulnerabilities (Cont.)

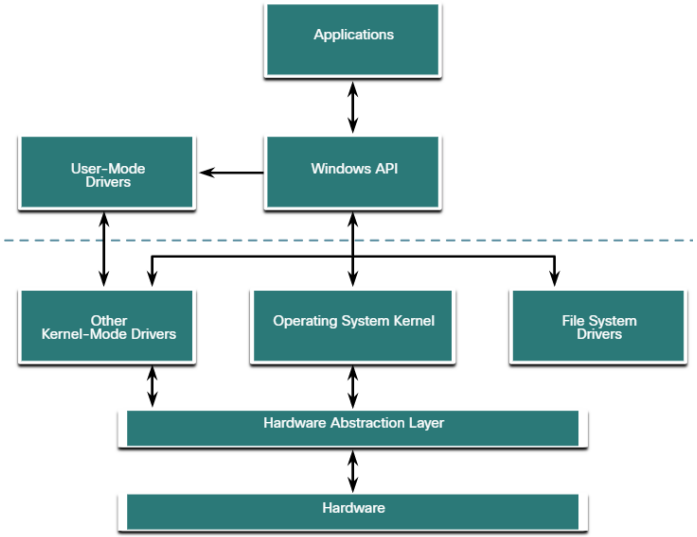
Some common Windows OS security recommendations include:

Recommendation	Description
Firewall	• By default, Windows uses Windows Firewall to limit communication with devices on the network. • Over time, rules may no longer apply. • For example, a port may be left open that should no longer be readily available. • It is important to review firewall settings periodically to ensure that the rules are still applicable and remove any that no longer apply.
File and share permissions	• These permissions must be set correctly. • It is easy to just give the “Everyone” group Full Control, but this allows all people to do what they want to all files. • It is best to provide each user or group with the minimum necessary permissions for all files and folders.
Weak or no password	• Many people choose weak passwords or do not use a password at all. • It is especially important to make sure that all accounts, especially the Administrator account, have a very strong password.
Login as Administrator	• When a user logs in as an administrator, any program they run will have the privileges of that account. • It is best to log in as a Standard User and only use the administrator password to accomplish certain tasks.

7.2 Windows Architecture and Operations

Hardware Abstraction Layer

Windows computers use many different types of hardware. The operating system can be installed on a purchased computer or on a computer that is assembled by the user. When the operating system is installed, it must be isolated from differences in hardware. The basic Windows architecture is shown in the figure.



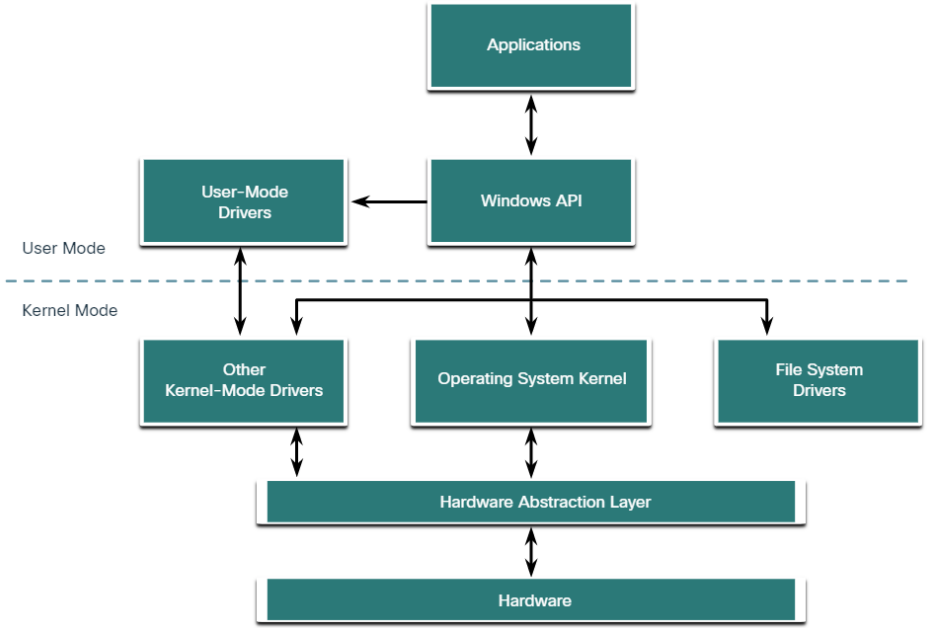
Hardware Abstraction Layer (Cont.)

A hardware abstraction layer (HAL) is software that handles all the communication between the hardware and the kernel. The kernel is the core of the operating system and has control over the entire computer. It handles all the input and output requests, memory, and peripherals connected to the computer.

In some instances, the kernel still communicates with the hardware directly, so it is not completely independent of the HAL. The HAL also needs the kernel to perform some functions.

User Mode and Kernel Mode

As identified in the figure, there are two different modes in which a CPU operates when the computer has Windows installed: the user mode and the kernel mode.



User Mode and Kernel Mode (Cont.)

- Installed applications run in user mode, and operating system code runs in kernel mode.
- Code that is executing in kernel mode has unrestricted access to the underlying hardware and can execute any CPU instruction.
- Kernel mode code also can reference any memory address directly.
- The code that runs in kernel mode uses the same address space and have no isolation from the operating system.
- When user mode code runs, it is granted its own restricted address space by the kernel, along with a process created specifically for the application.
- The reason for this functionality is mainly to prevent applications from changing operating system code that is running at the same time.

Windows File Systems

Windows File System	Description
exFAT	• This is a simple file system supported by many different operating systems. • FAT has limitations to the number of partitions, partition sizes, and file sizes that it can address, so it is not usually used for hard drives (HDs) or solid-state drives (SSDs) anymore. • Both FAT16 and FAT32 are available to use, with FAT32 being the most common because it has many fewer restrictions than FAT16.
Hierarchical File System Plus (HFS+)	• This file system is used on MAC OS X computers and allows much longer filenames, file sizes, and partition sizes than previous file systems. • Although it is not supported by Windows without special software, Windows is able to read data from HFS+ partitions.
Extended File System (EXT)	• This file system is used with Linux-based computers. • Although it is not supported by Windows, Windows is able to read data from EXT partitions with special software.
New Technology File System (NTFS)	• This is the most commonly used file system when installing Windows. All versions of Windows and Linux support NTFS. • Mac-OS X computers can only read an NTFS partition. They are able to write to an NTFS partition after installing special drivers.

Windows File Systems (Cont.)

NTFS is the most widely used file system for Windows for many reasons.

- Supports very large files and partitions and is very compatible with other operating systems
- Very reliable and supports recovery features
- Supports many security features

Before a storage device such as a disk can be used, it must be formatted with a file system. In turn, before a file system can be put into place on a storage device, the device needs to be partitioned.

- A hard drive is divided into areas called partitions.
- Each partition is a logical storage unit that can be formatted to store information, such as data files or applications.

Windows File Systems (Cont.)

NTFS formatting creates important structures on the disk for file storage, and tables for recording the locations of files:

- **Partition Boot Sector** - This is the first 16 sectors of the drive. It contains the location of the Master File Table (MFT). The last 16 sectors contain a copy of the boot sector.
- **Master File Table (MFT)** - This table contains the locations of all the files and directories on the partition, including file attributes such as security information and timestamps.
- **System Files** - These are hidden files that store information about other volumes and file attributes.
- **File Area** - The main area of the partition where files and directories are stored.

Note: When formatting a partition, the previous data may still be recoverable because not all the data is completely removed. The free space can be examined, and files can be retrieved which can compromise security. It is recommended to perform a secure wipe on a drive that is being reused. The secure wipe will write data to the entire drive multiple times to ensure there is no remaining data.

Alternate Data Streams

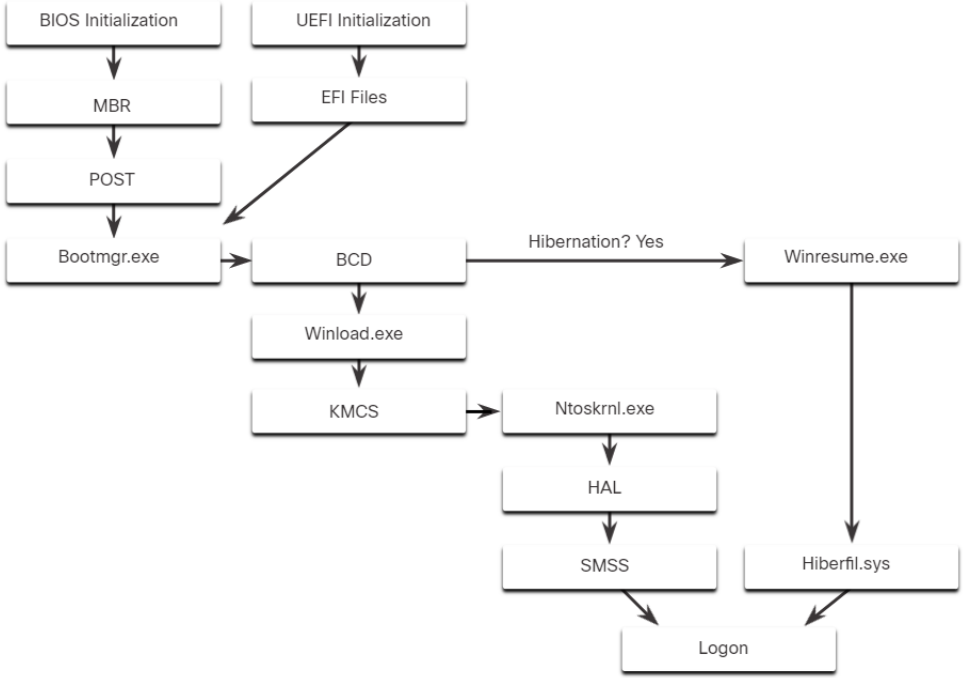
```
C:\ADS> echo "Alternate Data Here" > Testfile.txt:ADS
C:\ADS> dir
 Volume in drive C is Windows
 Volume Serial Number is A606-CB1B
 Directory of C:\ADS
2020-04-28  04:01 PM    <DIR>          .
2020-04-28  04:01 PM    <DIR>          ..
2020-04-28  04:01 PM                 0 Testfile.txt
               1 File(s)              0 bytes
               2 Dir(s)  43,509,571,584 bytes free
C:\ADS> more < Testfile.txt:ADS
"Alternate Data Here"
C:\ADS> dir /r
 Volume in drive C is Windows
 Volume Serial Number is A606-CB1B
 Directory of C:\ADS
2020-04-28  04:01 PM    <DIR>          .
2020-04-28  04:01 PM    <DIR>          ..
2020-04-28  04:01 PM                 0 Testfile.txt
                                    24 Testfile.txt:ADS:$DATA
               1 File(s)              0 bytes
               2 Dir(s)  43,509,624,832 bytes free
C:\ADS>
```

NTFS stores files as a series of attributes, such as the name of the file, or a timestamp. The data which the file contains is stored in the attribute $DATA and is known as a data stream. By using NTFS, you can connect Alternate Data Streams (ADSs) to the file.

In the NTFS file system, a file with an ADS is identified after the filename and a colon, for example, Testfile.txt:ADS. This filename indicates an ADS is associated with the file called Testfile.txt. An example of an ADS is shown in the command output.

Windows Boot Process

Many actions occur between the time that the computer power button is pressed, and Windows is fully loaded, as shown in the figure. This is known as the Windows Boot process.



Windows Boot Process (Cont.)

Two types of computer firmware exist:

- **Basic Input-Output System (BIOS):** BIOS firmware was created in the early 1980s and works in the same way it did when it was created. As computers evolved, it became difficult for BIOS firmware to support all the new features requested by users.

- **Unified Extensible Firmware Interface (UEFI):** UEFI was designed to replace BIOS and support the new features.

Windows Boot Process (Cont.)

BIOS firmware boot process:

- The process begins with the BIOS initialization phase - this is when hardware devices are initialized and a power on self-test (POST) is performed to make sure these devices are communicating.
- When the system disk is discovered, the POST ends.
- The last instruction in the POST is to look for the master boot record (MBR).
- The MBR contains a small program that is responsible for locating and loading the operating system.
- The BIOS executes this code, and the operating system starts to load.

UEFI firmware boot process:

- UEFI boots by loading EFI program files, stored as .efi files in a special disk partition, known as the EFI System Partition (ESP).

Windows Boot Process (Cont.)

Boot process for BIOS or UEFI after a valid windows installation is located:

- The Bootmgr.exe file is run.
- Bootmgr.exe reads the Boot Configuration Database (BCD)
  - The BCD contains any additional code needed to start the computer, along with an indication of whether the computer is coming out of hibernation, or if this is a cold start.
- If the computer is coming out of hibernation, the boot process continues with Winresume.exe.
  - This allows the computer to read the Hiberfil.sys file which contains the state of the computer when it was put into hibernation.
- If the computer is being booted from a cold start, then the Winload.exe file is loaded.
  - The Winload.exe file creates a record of the hardware configuration in the registry.
  - The registry is a record of the settings, options, hardware, and software the computer has.
- After the drivers have been examined, Winload.exe runs Ntoskrnl.exe which starts the Windows kernel and sets up the HAL.
- The Session Manager Subsystem (SMSS) reads the registry to create the user environment, start the Winlogon service, and prepare each user's desktop as they log on.

Windows Startup

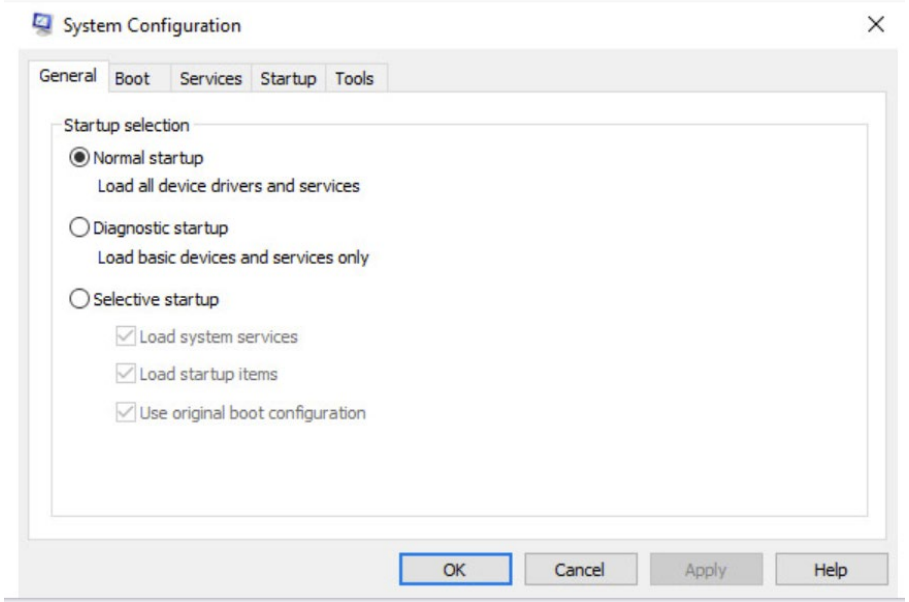
- There are two important registry items that are used to automatically start applications and services:
  - **HKEY_LOCAL_MACHINE** - Several aspects of Windows configuration are stored in this key, including information about services that start with each boot.
  - **HKEY_CURRENT_USER** - Several aspects related to the logged in user are stored in this key, including information about services that start only when the user logs on to the computer.

- Different entries in these registry locations define which services and applications will start, as indicated by their entry type.

- These types include Run, RunOnce, RunServices, RunServicesOnce, and Userinit.

Windows Startup (Cont.)

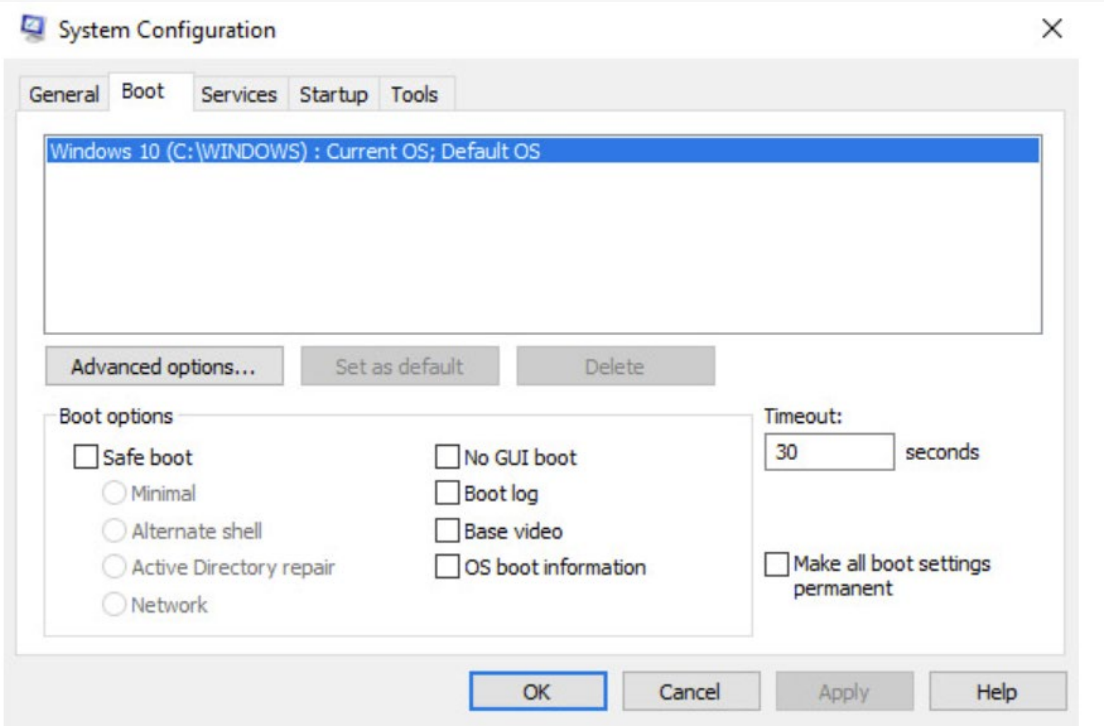
The Msconfig tool opens the System Configuration window. There are five tabs which contain the configuration options: **General, Boot, Services, Startup, and Tools.**



General: Three different startup types can be chosen here.

- Normal loads all drivers and services.
- Diagnostic loads only basic drivers and services.
- Selective allows the user to choose what to load on startup.

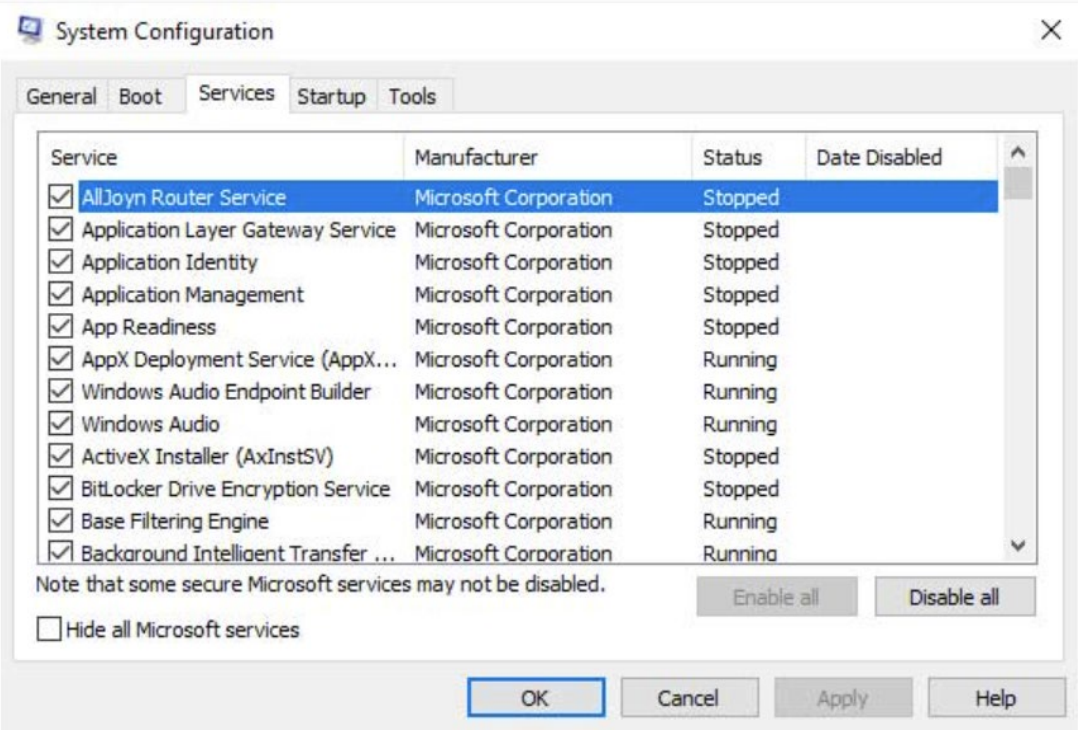
Windows Startup (Cont.)



Boot: Any installed operating system can be chosen here to start.

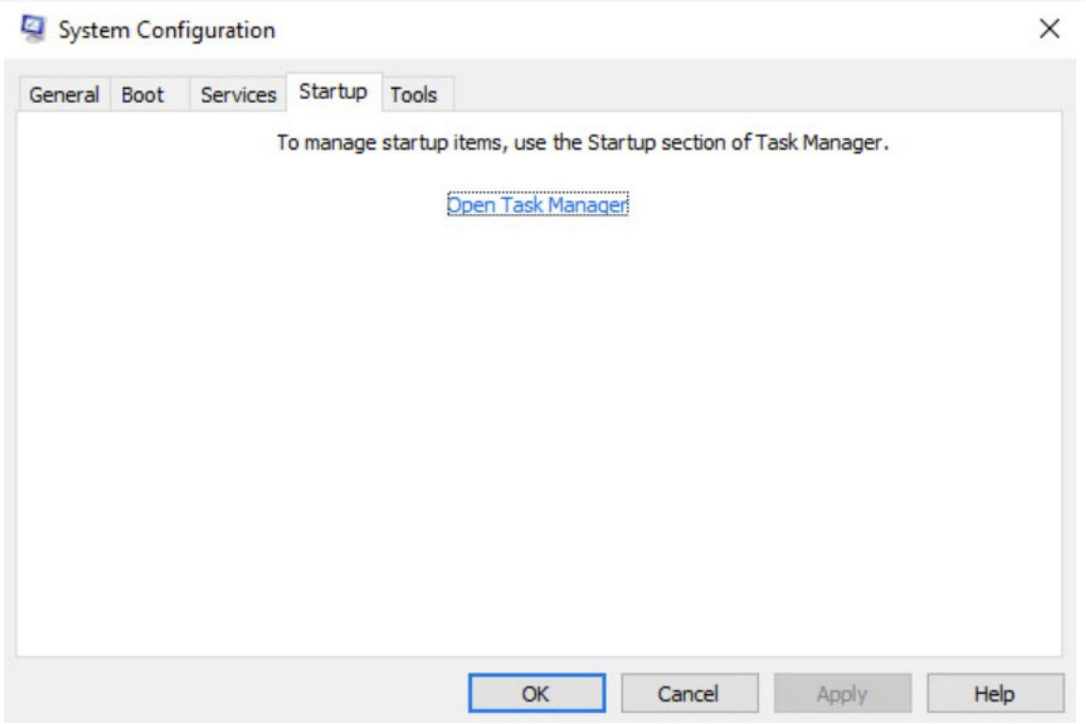
There are also options for Safe boot, which is used to troubleshoot startup.

Windows Startup (Cont.)



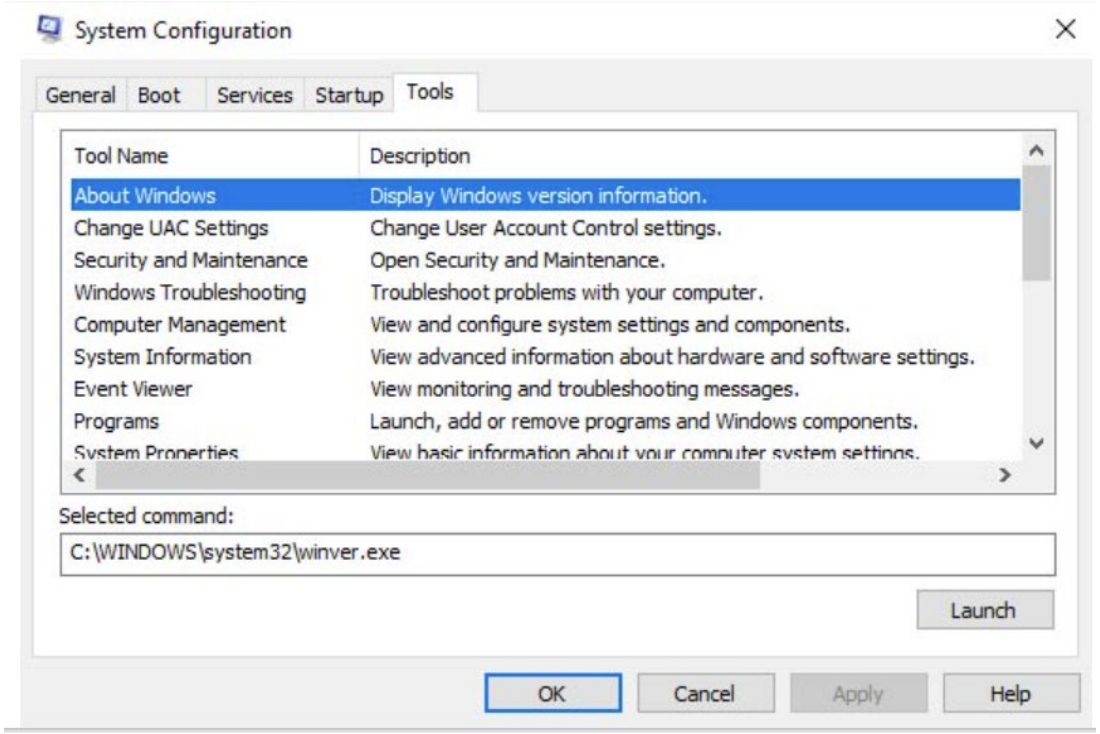
Services: All the installed services are listed here so that they can be chosen to start at startup.

Windows Startup (Cont.)



Startup: All the applications and services that are configured to automatically begin at startup can be enabled or disabled by opening the task manager from this tab.

Windows Startup (Cont.)



Tools: Many common operating system tools can be launched directly from this tab.

Windows Shutdown

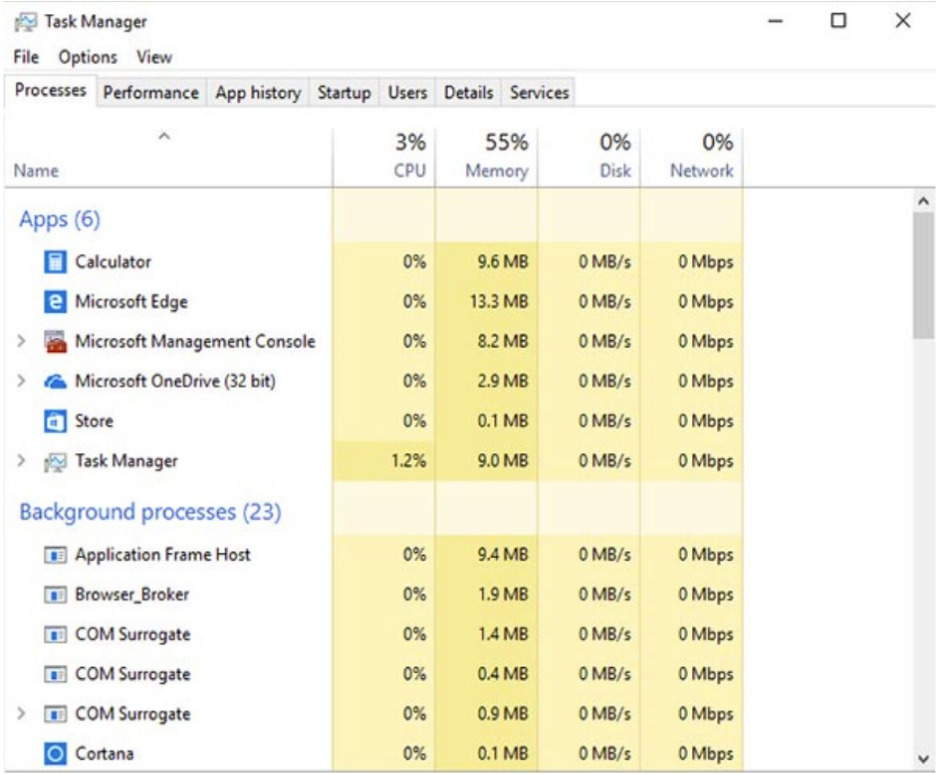
- It is always best to perform a proper shutdown to turn off the computer.
  - Files that are left open, services that are closed out of order, and applications that hang can all be damaged if the power is turned off without first informing the operating system.
  - During shutdown, the computer will close user mode applications first, followed by kernel mode processes.

- There are several ways to shut down a Windows computer: Start menu power options, the command line command shutdown, and using Ctrl+Alt+Delete then clicking the power icon.

Three options for shutting down the computer include:

- **Shutdown** - Turns the computer off (power off).
- **Restart** - Re-boots the computer (power off then power on).
- **Hibernate** - Records the current state of the computer and user environment and stores it in a file. Hibernation allows users to pick up right where they left off very quickly with all their files and programs still open.

Processes, Threads, and Services

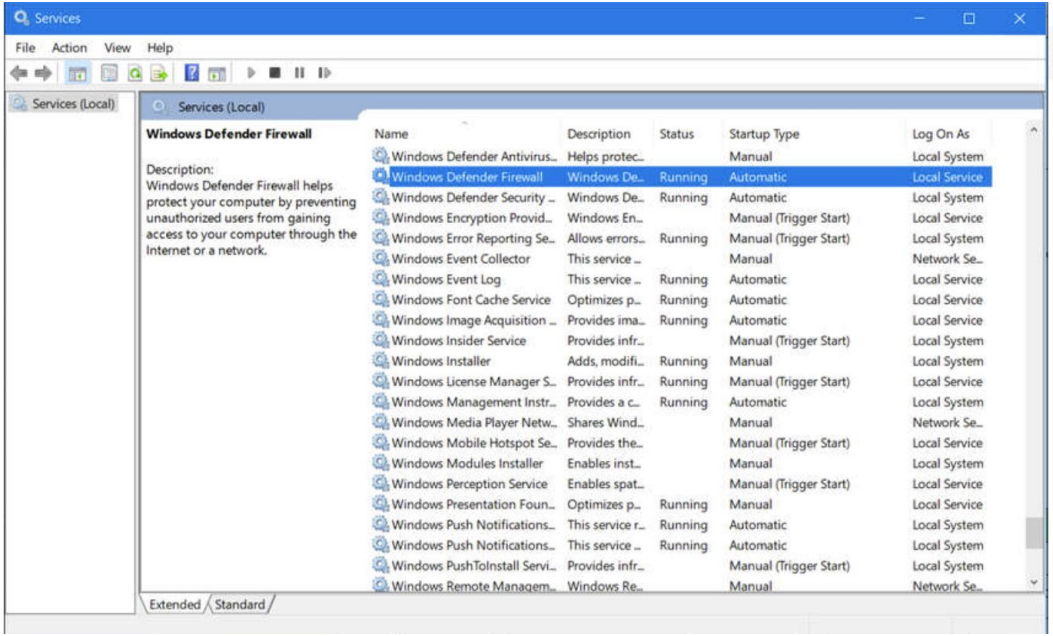


A Windows application is made up of processes. The application can have one or many processes dedicated to it. A process is any program that is currently executing.

Each process that runs is made up of at least one thread. A thread is a part of the process that can be executed. The processor performs calculations on the thread.

To configure Windows processes, search for Task Manager. The Processes tab of the Task Manager is shown in the figure.

Processes, Threads, and Services (Cont.)



The threads dedicated to a process are contained within the same address space. This prevents the corruption of other processes. Because Windows multitasks, multiple threads can be executed at the same time.

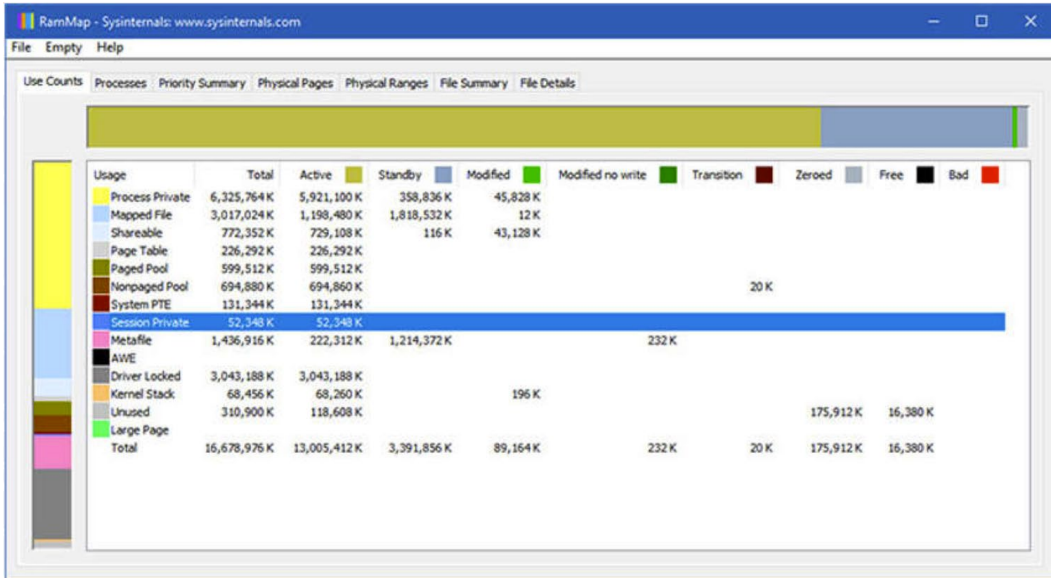
Some of the processes that Windows runs are services. Services provide long-running functionality, such as wireless or access to an FTP server.

Memory Allocation and Handles

- A computer works by storing instructions in RAM until the CPU processes them.
- The virtual address space for a process is the set of virtual addresses that the process can use.
  - Each process in a 32-bit Windows computer supports a virtual address space that enables addressing up to 4 gigabytes.
  - Each process in a 64-bit Windows computer supports a virtual address space of 8 terabytes.

- Each user space process runs in a private address space, separate from other user space processes.
  - When the user space process needs to access kernel resources, it must use a process handle.
  - The process handle provides the access needed by the user space process without a direct connection to kernel resource.

Memory Allocation and Handles (Cont.)



A powerful tool for viewing memory allocation is RAMMap, which is shown in the figure.

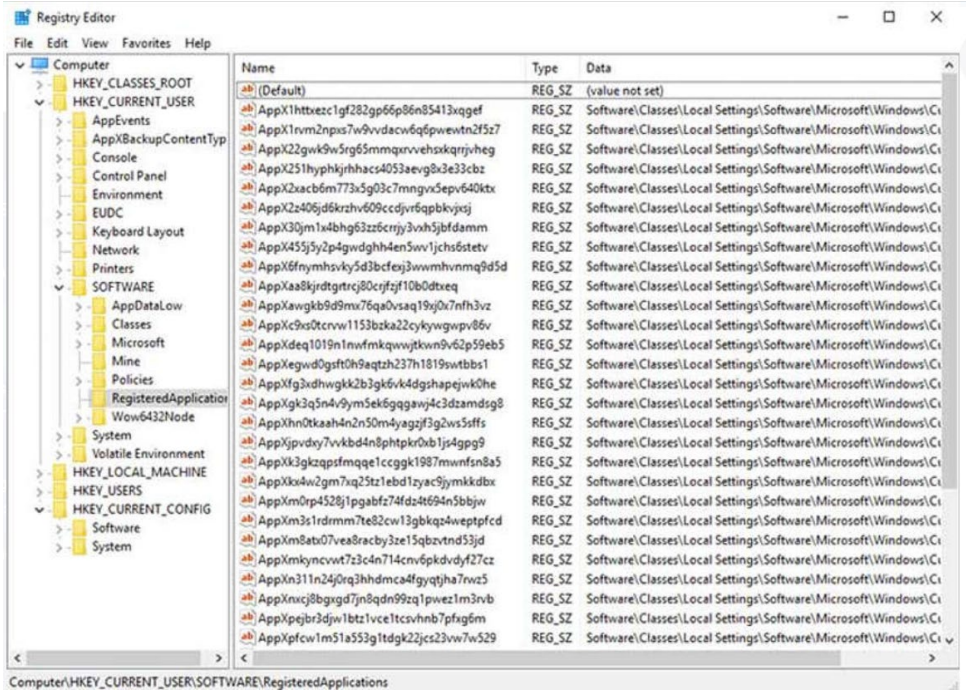
RAMMap provides a wealth of information regarding how Windows has allocated system memory to the kernel, processes, drivers, and applications.

The Windows Registry

Windows stores the information about hardware, applications, users, and system settings in a large database known as the registry. The ways that these objects interact are also recorded, such as what files an application opens and the property details of folders and applications. The registry is a hierarchical database where the highest level is known as a hive, below that there are keys, followed by subkeys. Values store data and are stored in the keys and subkeys. A registry key can be up to 512 levels deep.

Registry Hive	Description
HKEY_CURRENT_USER (HKCU)	Holds information concerning the currently logged in user.
HKEY_USERS (HKU)	Holds information concerning all the user accounts on the host.
HKEY_CLASSES_ROOT (HKCR)	Holds information about object linking and embedding (OLE) registrations. OLE allows users to embed objects from other applications (like a spreadsheet) into a single document (like a Word document).
HKEY_LOCAL_MACHINE (HKLM)	Holds system-related information.
HKEY_CURRENT_CONFIG (HKCC)	Holds information about the current hardware profile.

The Windows Registry (Cont.)



New hives cannot be created. The registry keys and values in the hives can be created, modified, or deleted by an account with administrative privileges.

As shown in the figure, the tool **regedit.exe** is used to modify the registry. Be very careful when using this tool. Minor changes to the registry can have massive or even catastrophic effects.

The Windows Registry (Cont.)

- Use the left panel to navigate the hives and the structure below it and use the right panel to see the contents of the highlighted item in the left panel.

- Registry keys can contain either a subkey or a value. The different values that keys can contain are as follows:
  - **REG_BINARY** - Numbers or Boolean values
  - **REG_DWORD** - Numbers greater than 32 bits or raw data
  - **REG_SZ** - String values

- Because the registry holds almost all the operating system and user information, it is critical to make sure that it does not become compromised.
  - Potentially malicious applications can add registry keys so that they start when the computer is started.

- Registry contains activity that a user performs during normal day-to-day computer use.
  - This includes the history of hardware devices, all devices that have been connected to the computer, name, manufacturer, and serial number.

Lab - Exploring Processes, Threads, Handles, and Windows Registry

In this lab, you will explore the processes, threads, and handles using Process Explorer in the SysInternals Suite. You will also use the Windows Registry to change a setting.

Part 1: Exploring Processes
Part 2: Exploring Threads and Handles
Part 3: Exploring Windows Registry

7.3 Windows Configuration and Monitoring

Run as Administrator

net localgroup /?

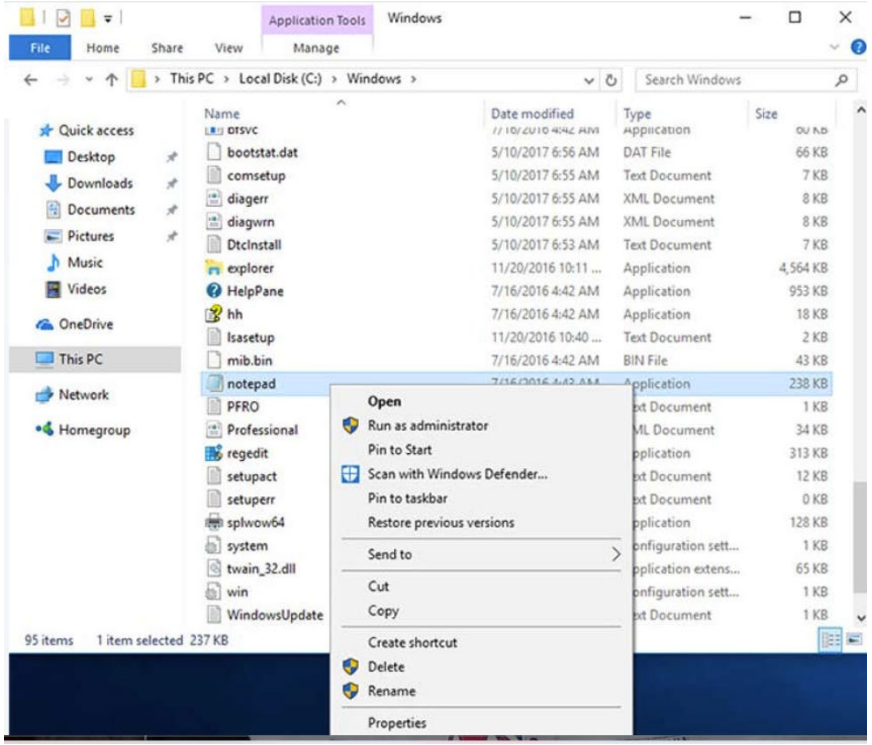
As a security best practice, it is not advisable to log on to Windows using the Administrator account or an account with administrative privileges.

- Any program that is executed while logged on with those privileges will inherit administrative privileges.
- Malware that has administrative privileges has full access to all the files and folders on the computer.

Run as Administrator (Cont.)

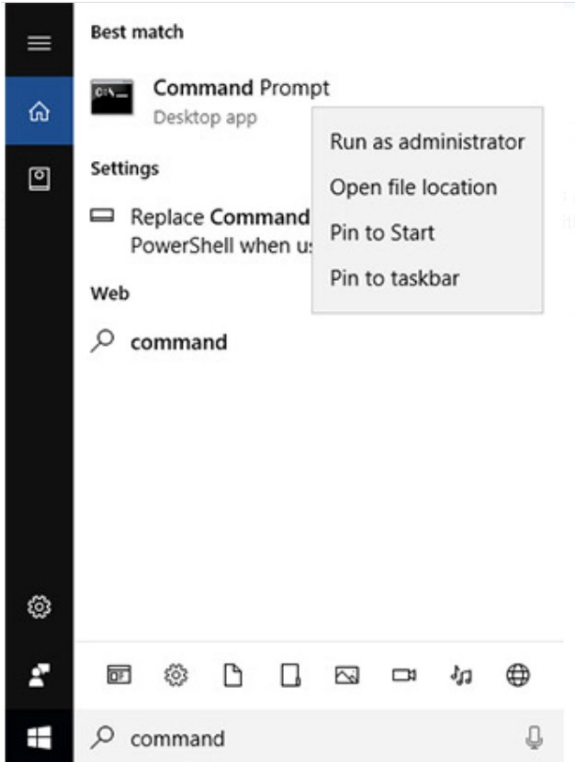
Sometimes, it is necessary to run or install software that requires the privileges of the Administrator. To accomplish this, there are two different ways to install it.

Administrator: Right-click the command in the Windows File Explorer and choose Run as Administrator from the Context Menu.



Run as Administrator (Cont.)

Administrator Command Prompt: Right-click the command in the Windows File Explorer and choose Run as Administrator from the Context Menu.



Local Users and Domains

- When you start a new computer for the first time, or you install Windows, you will be prompted to create a user account (local user).
  - This contains your customization settings, access permissions, file locations, and many other user-specific data.

- As a security best practice, do not enable the Administrator account and do not give standard users administrative privileges.

- The Guests account should not be enabled.

- To make administration of users easier, Windows uses groups.
  - A group will have a name and a specific set of permissions associated with it.
  - When a user is placed into a group, the permissions of that group are given to that user.

- Windows can also use domains to set permissions.
  - A domain is a type of network service where the users, groups, computers, peripherals, and security settings are stored on and controlled by a database.

CLI and PowerShell

- The Windows command line interface (CLI) can be used to run programs, navigate the file system, and manage files and folders.
- To open the Windows CLI, search for **cmd.exe** and click the program.

The prompt displays the current location within the file system. A few things to remember:

- The file names and paths are not case-sensitive, by default.
- Storage devices are assigned a letter for reference. The drive letter is followed by a colon and backslash (\). This indicates the root, or highest level, of the device.
- Commands that have optional switches use the forward slash (/) to delineate between the command and the switch option.
- You can use the Tab key to auto-complete commands when directories or files are referenced.
- Windows keeps a history of the commands that were entered during a CLI session. Access previously entered commands by using the up and down arrow keys.
- To switch between storage devices, type the letter of the device, followed by a colon, and then press Enter.

CLI and PowerShell (Cont.)

- CLI cannot work together with the core of Windows or the GUI.
- Windows PowerShell can be used to create scripts to automate tasks that the regular CLI is unable to create.

These are the types of commands that PowerShell can execute:

- **cmdlets** - These commands perform an action and return an output or object to the next command that will be executed.
- **PowerShell scripts** - These are files with a **.ps1** extension that contain PowerShell commands that are executed.
- **PowerShell functions** - These are pieces of code that can be referenced in a script.

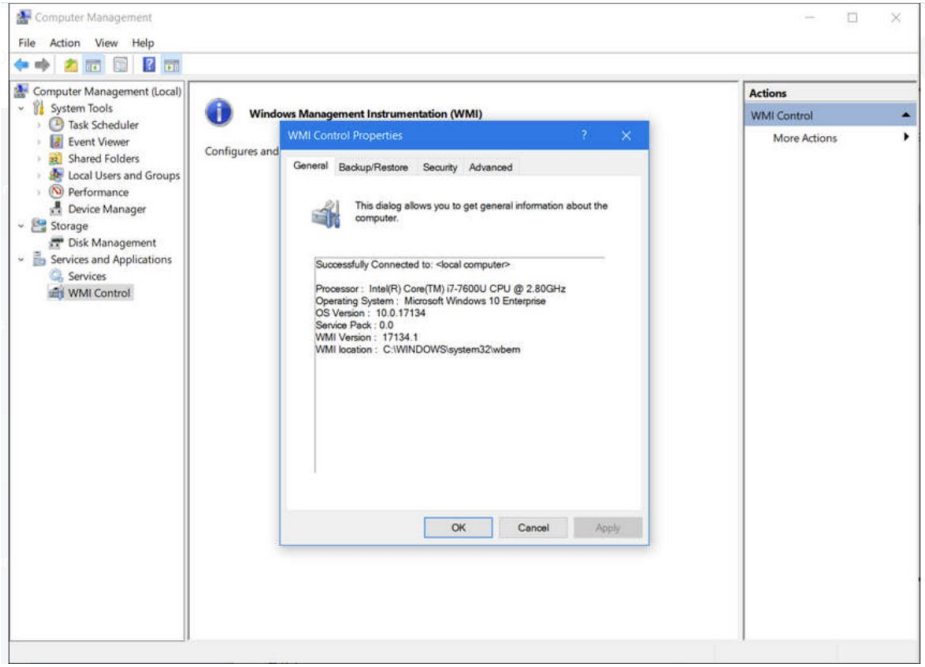
CLI and PowerShell (Cont.)

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\WINDOWS\system32> help
TOPIC
    Windows PowerShell Help System
SHORT DESCRIPTION
    Displays help about Windows PowerShell cmdlets and concepts.
LONG DESCRIPTION
    Windows PowerShell Help describes Windows PowerShell cmdlets,
    functions, scripts, and modules, and explains concepts, including
    the elements of the Windows PowerShell language.
    Windows PowerShell does not include help files, but you can read the
    help topics online, or use the Update-Help cmdlet to download help files
    to your computer and then use the Get-Help cmdlet to display the help
    topics at the command line.
    You can also use the Update-Help cmdlet to download updated help files
    as they are released so that your local help content is never obsolete.
    Without help files, Get-Help displays auto-generated help for cmdlets,
    functions, and scripts.
  ONLINE HELP
    You can find help for Windows PowerShell online in the TechNet Library
    beginning at http://go.microsoft.com/fwlink/?LinkID=108518.
```

There are four levels of help in Windows PowerShell:

- **get-help** *PS command* - Displays basic help for a command
- **get-help** *PS command [-examples]* - Displays basic help for a command with examples
- **get-help** *PS command [-detailed]* - Displays detailed help for a command with examples
- **get-help** *PS command [-full]* - Displays all help information for a command with examples in greater depth

Windows Management Instrumentation



Windows Management Instrumentation (WMI) is used to manage remote computers. It can retrieve information about computer components, hardware and software statistics, and monitor the health of remote computers.

To open the WMI control from the Control Panel, double-click **Administrative Tools > Computer Management** to open the Computer Management window, expand the **Services and Applications** tree and right-click the **WMI Control icon > Properties**.

The WMI Control Properties window is shown in the figure.

Windows Management Instrumentation (Cont.)

These are the four tabs in the WMI Control Properties window:

- **General** - Summary information about the local computer and WMI
- **Backup/Restore** - Allows manual backup of statistics gathered by WMI
- **Security** - Settings to configure who has access to different WMI statistics
- **Advanced** - Settings to configure the default namespace for WMI

- Some attacks today use WMI to connect to remote systems, modify the registry, and run commands.
- WMI helps them to avoid detection because it is common traffic, most often trusted by the network security devices and the remote WMI commands do not usually leave evidence on the remote host.

The net Command

ติดต่อข้างนอก

```
C:\> net help
The syntax of this command is:
NET HELP
command
     -or-
NET command /HELP
  Commands available are:
  NET ACCOUNTS             NET HELPMSG              NET STATISTICS
  NET COMPUTER             NET LOCALGROUP           NET STOP
  NET CONFIG               NET PAUSE                NET TIME
  NET CONTINUE             NET SESSION              NET USE
  NET FILE                 NET SHARE                NET USER
  NET GROUP                NET START                NET VIEW
  NET HELP
  NET HELP NAMES explains different types of names in NET HELP syntax lines.
  NET HELP SERVICES lists some of the services you can start.
  NET HELP SYNTAX explains how to read NET HELP syntax lines.
  NET HELP command | MORE displays Help one screen at a time.
C:\>
```

- One important command is the **net** command, which is used in the administration and maintenance of the OS.
- The **net** command supports many subcommands that follow the **net** command and can be combined with switches to focus on specific output.

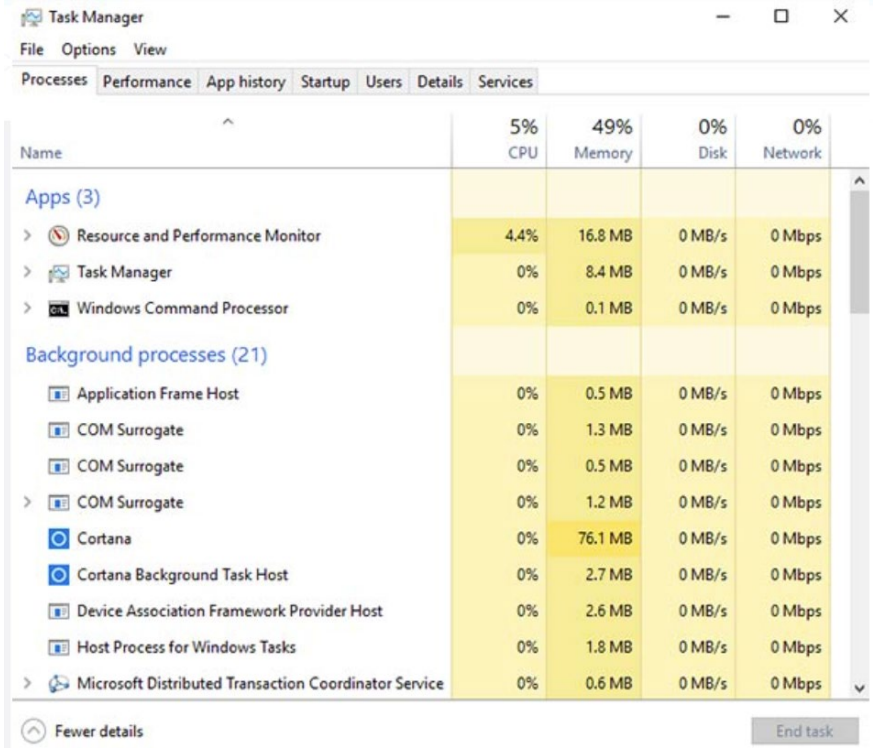
The net Command (Cont.)

Common net commands:

Command	Description
net accounts	Sets password and logon requirements for users
net session	Lists or disconnects sessions between a computer and other computers on the network
net share	Creates, removes, or manages shared resources
net start	Starts a network service or lists running network services
net stop	Stops a network service
net use	Connects, disconnects, and displays information about shared network resources
net view	Shows a list of computers and network devices on the network

wmic

Task Manager and Resource Monitor



There are two very important and useful tools to help an administrator to understand the many different applications, services, and processes that are running on a Windows computer.

Task Manager

The Task Manager, which is shown in the figure, provides a lot of information about the software that is running and the general performance of the computer.

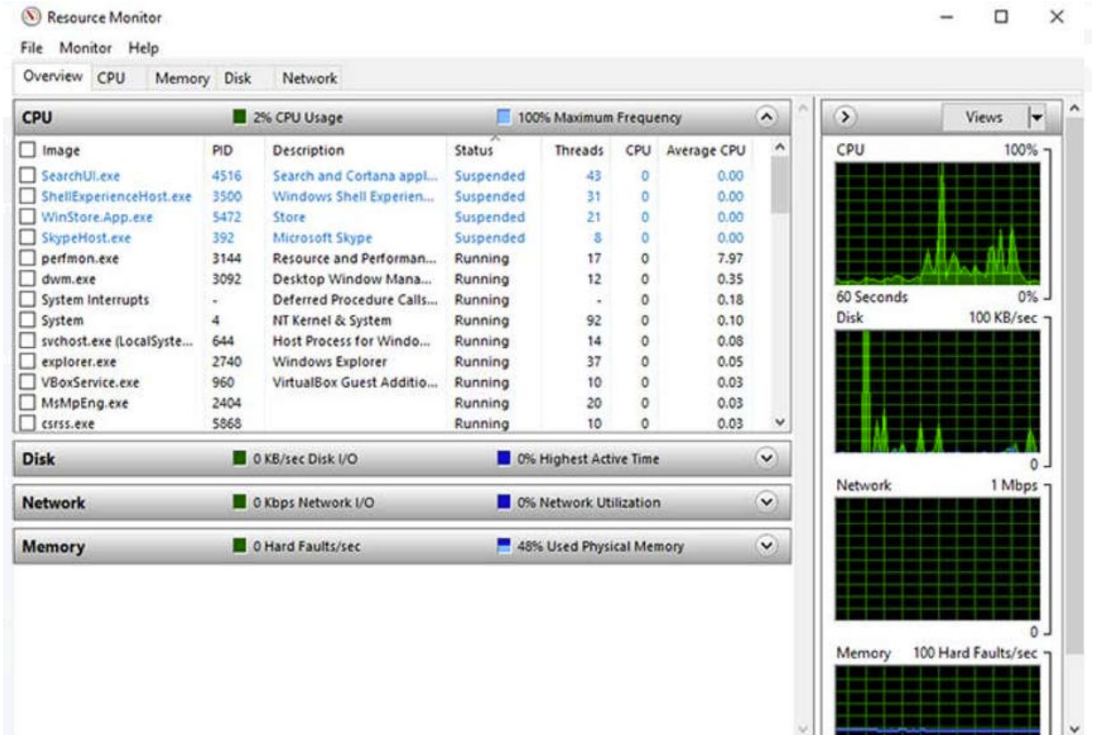
Task Manager and Resource Monitor (Cont.)

Task Manager Tabs	Description
Processes	• Lists all the programs and processes that are currently running. • Displays the CPU, memory, disk, and network utilization of each process. • The properties of a process can be examined or ended if it is not behaving properly or has stalled.
Performance	• A view of all the performance statistics provides a useful overview of the CPU, memory, disk, and network performance. • Clicking each item in the left pane will show detailed statistics of that item in the right pane.
App history	• The use of resources by application over time provides insight into applications that are consuming more resources than they should. • Click Options and Show history for all processes to see the history of every process that has run since the computer was started.
Startup	• All the applications and services that start when the computer is booted are shown in this tab. • To disable a program from starting at startup, right-click the item and choose Disable.

Task Manager and Resource Monitor (Cont.)

Task Manager Tabs	Description
Users	• All the users that are logged on to the computer are shown in this tab. • Also shown are all the resources that each user's applications and processes are using. • From this tab, an administrator can disconnect a user from the computer.
Details	• Similar to the Processes tab, this tab provides additional management options for processes such as setting a priority to make the processor devote more or less time to a process. • CPU affinity can also be set which determines which core or CPU a program will use. • Also, a useful feature called Analyze wait chain shows any process for which another process is waiting. • This feature helps to determine if a process is simply waiting or is stalled.
Services	• All the services that are loaded are shown in this tab. • The process ID (PID) and a short description are also shown along with the status of either Running or Stopped. • At the bottom, there is a button to open the Services console which provides additional management of services.

Task Manager and Resource Monitor (Cont.)



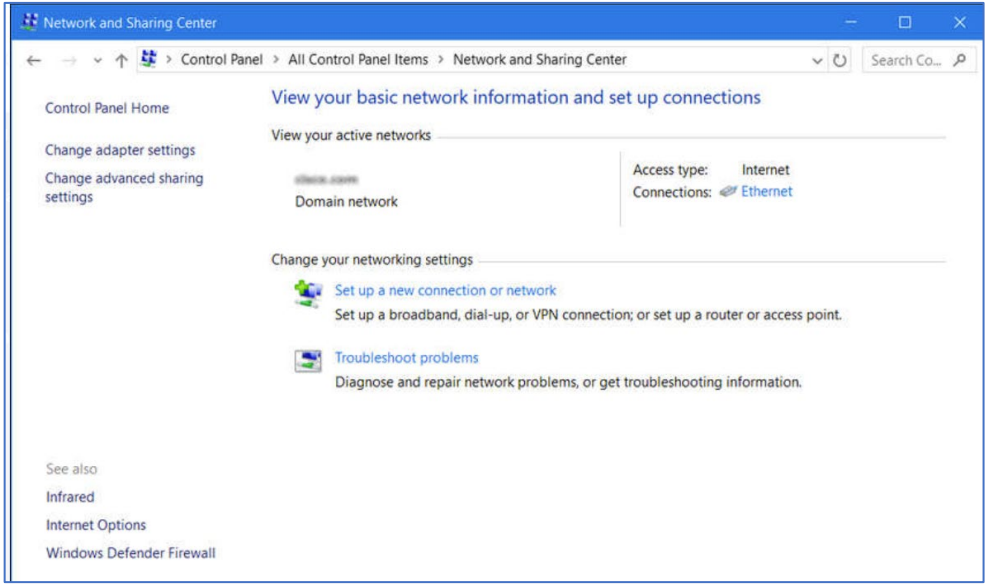
When more detailed information about resource usage is needed, you can use the **Resource Monitor**, as shown in the figure.

Task Manager and Resource Monitor (Cont.)

Resource Monitor can help find the source of the problem when your computer is acting erratically.

Resource Monitor Tabs	Description
Overview	• The tab displays the general usage for each resource.
CPU	• The PID, number of threads, which CPU the process is using, and the average CPU usage of each process is shown. • Additional information about any services that the process relies on, and the associated handles and modules can be seen by expanding the lower rows.
Memory	• All the statistical information about how each process uses memory is shown in this tab. • Also, an overview of usage of all the RAM is shown below the Processes row.
Disk	• All the processes that are using a disk are shown in this tab, with read/write statistics and an overview of each storage device.
Network	• All the processes that are using the network are shown in this tab, with read/write statistics. • Most importantly, the current TCP connections are shown, along with all of the ports that are listening. • This tab is very useful when trying to determine which applications and processes are communicating over the network. • It makes it possible to tell if an unauthorized process is accessing the network, listening for a communication, and the address with which it is communicating.

Networking



- One of the most important features of any operating system is the ability for the computer to connect to a network
- Without this feature, there is no access to network resources or the internet
- To configure Windows networking properties and test networking settings, the **Network and Sharing Center** is used
- This view shows whether there is internet access and if the network is private, public, or guest.

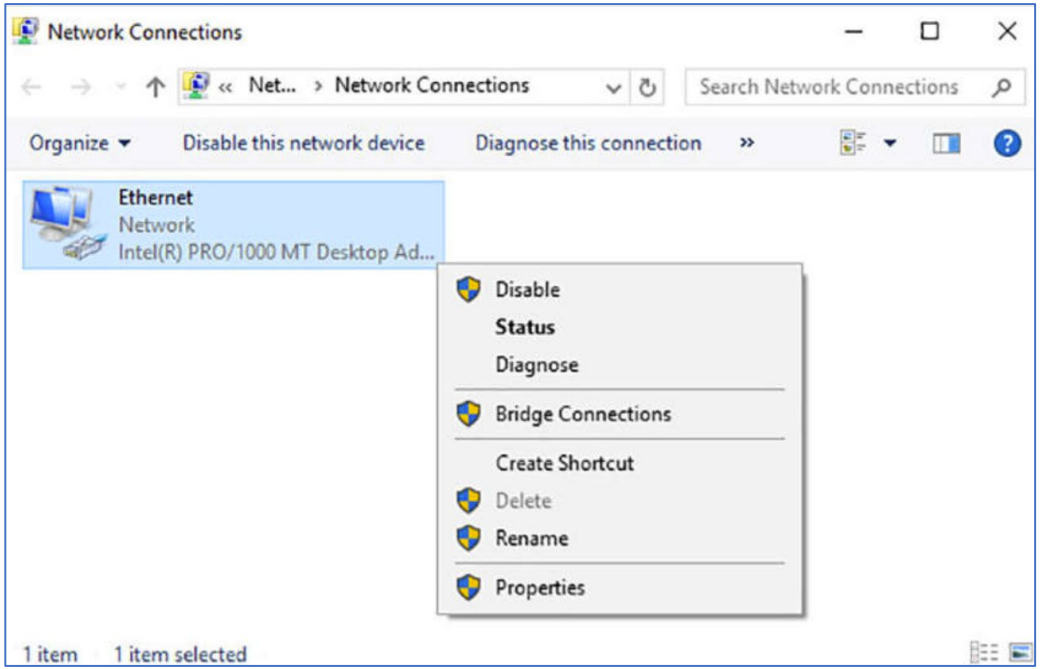
Networking (Cont.)

Change Adapter Settings

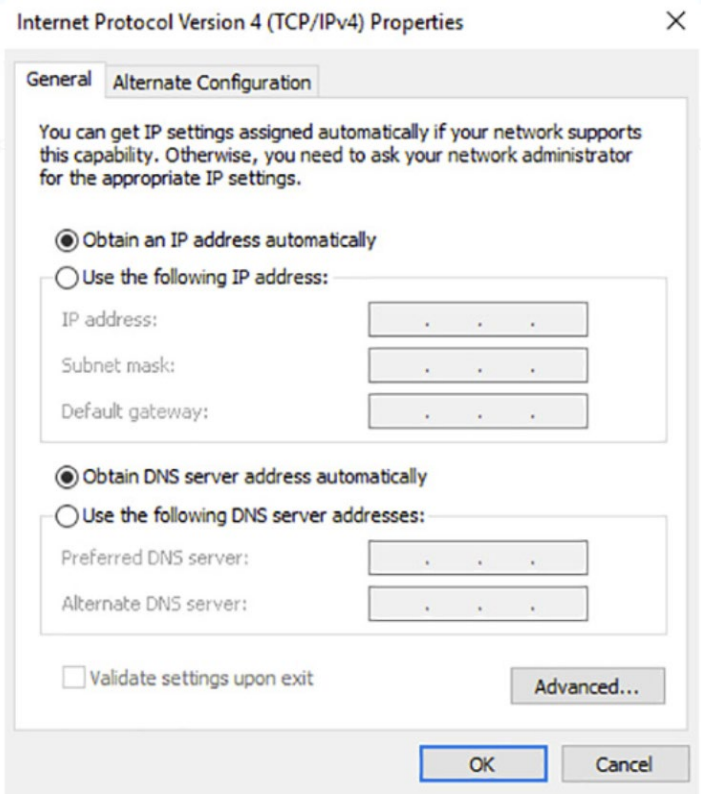
- To configure a network adapter, choose Change adapter settings in the Networking and Sharing Center to show the network connections that are available.
- Select the adapter that you want to configure.
- In this case, we change an Ethernet adapter to acquire its IPv4 address automatically from the network.

Networking (Cont.)

Access Adapter Properties: Right-click the adapter you wish to configure and choose Properties, as shown in the figure.



Networking (Cont.)



Access TCP/IPV4 Properties:

This connection uses the following items: **Internet Protocol Version 4 (TCP/IPv4)** or **Internet Protocol Version 6 (TCP/IPv6)** depending on which version you wish to use. In the figure, IPv4 is being selected.

Networking (Cont.)

netstat -abno

nslookup and netstat

- Domain Name System (DNS) should also be tested because it is essential to finding the address of hosts by translating it from a name, such as a URL.
- Use the **nslookup** command to test DNS.
- Type **nslookup cisco.com** at the command prompt to find the address of the Cisco webserver.

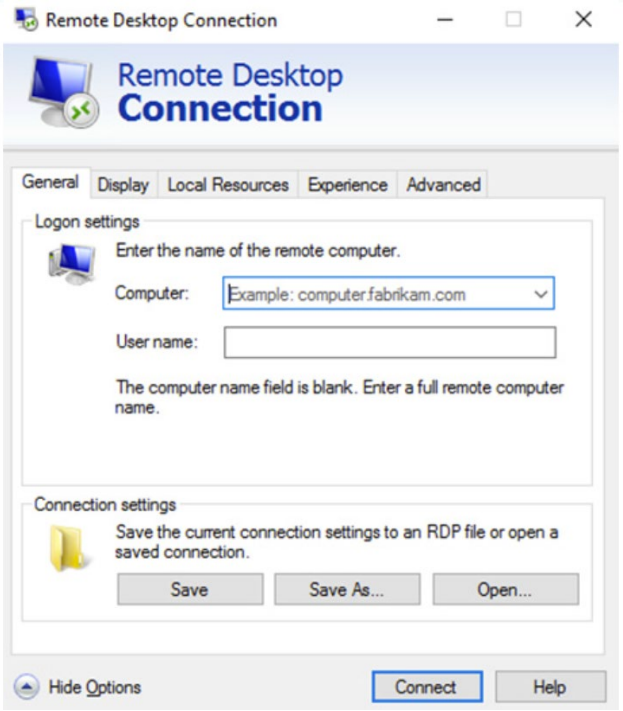
```
C:\Users\USER>netstat
Active Connections
  Proto     Local Address         Foreign Address     State
  TCP     127.0.0.1:3030        USER-VGFFA:58652   ESTABLISHED
  TCP     127.0.0.1:3030        USER-VGFFA:62114   ESTABLISHED
  TCP     &127.0.0.1:3030       USER-VGFFA:62480   TIME_WAIT
  TCP     127.0.0.1:3030        USER-VGFFA:62481   TIME_WAIT
  TCP     127.0.0.1:3030        USER-VGFFA:62484   TIME_WAIT
```

Accessing Network Resources

- Windows uses networking for many different applications such as web, email, and file services. Microsoft aided in the development of the Server Message Block (SMB) protocol to share network resources.
  - SMB is mostly used for accessing files on remote hosts
  - The Universal Naming Convention (UNC) format is used to connect to resources, for example: \\servername\sharename\file
  - servername is the server that is hosting the resource
  - sharename is the root of the folder in the file system on the remote host
  - file is the resource that the local host is trying to find

- When sharing resources on the network, the area of the file system that will be shared will need to be identified.

Accessing Network Resources (Cont.)



- To connect to a share, type the UNC of the share into the Windows File Explorer
- You will be asked to provide credentials for accessing the resource.
- You can log in to a remote host to make configuration changes, install software, or troubleshoot an issue.
  - In Windows, this feature uses the Remote Desktop Protocol (RDP).
  - To start RDP and connect to a remote computer, search for remote desktop and click the application. **The Remote Desktop Connection window is shown in the figure.**
  - RDP is designed to permit remote users to control individual hosts, therefore, it is a natural target for threat actors.

Windows Server

- Most Windows installations are performed as desktop installations on desktops and laptops.
- There is another edition of Windows that is mainly used in data centers called Windows Server.
  - This is a family of Microsoft products that began with Windows Server 2003.
  - Windows Server hosts many different services and can fulfill different roles within a company.

These are some of the services that Windows Server provides:

- **Network Services** - DNS, DHCP, Terminal services, Network Controller, and Hyper-V Network virtualization
- **File Services** - SMB, NFS, and DFS
- **Web Services** - FTP, HTTP, and HTTPS
- **Management** - Group policy and Active Directory domain services control

Lab - Create User Accounts

In this lab, you will create and modify user accounts in Windows.

- Part 1: Creating a New Local User Account
- Part 2: Reviewing User Account Properties
- Part 3: Modifying Local User Accounts

Lab - Using Windows PowerShell

In this lab, you will explore some of the functions of PowerShell.

- Part 1: Access PowerShell console
- Part 2: Explore Command Prompt and PowerShell commands
- Part 3: Explore cmdlets
- Part 4: Explore the netstat command using PowerShell
- Part 5: Empty recycle bin using PowerShell

Lab - Windows Task Manager

In this lab, you will explore Task Manager and manage processes from within Task Manager.

- Part 1: Working in the Processes tab
- Part 2: Working in the Services tab
- Part 3: Working in the Performance tab

Lab - Monitor and Manage System Resources in Windows

In this lab, you will use administrative tools to monitor and manage Windows system resources.

- Part 1: Starting and Stopping the Routing and Remote Access service
- Part 2: Working in the Computer Management Utility
- Part 3: Configuring Administrative Tools

7.4 Windows Security

The netstat Command

- When malware is present in a computer, it will often open communication ports on the host to send and receive data. The **netstat** command can be used to look for inbound or outbound connections that are not authorized. When used on its own, the **netstat** command will display all the active TCP connections.

- By examining these connections, it is possible to determine which of the programs are listening for connections that are not authorized. When a program is suspected of being malware, a little research can be performed to determine its legitimacy. From there, the process can be shut down with Task Manager, and malware removal software can be used to clean the computer.

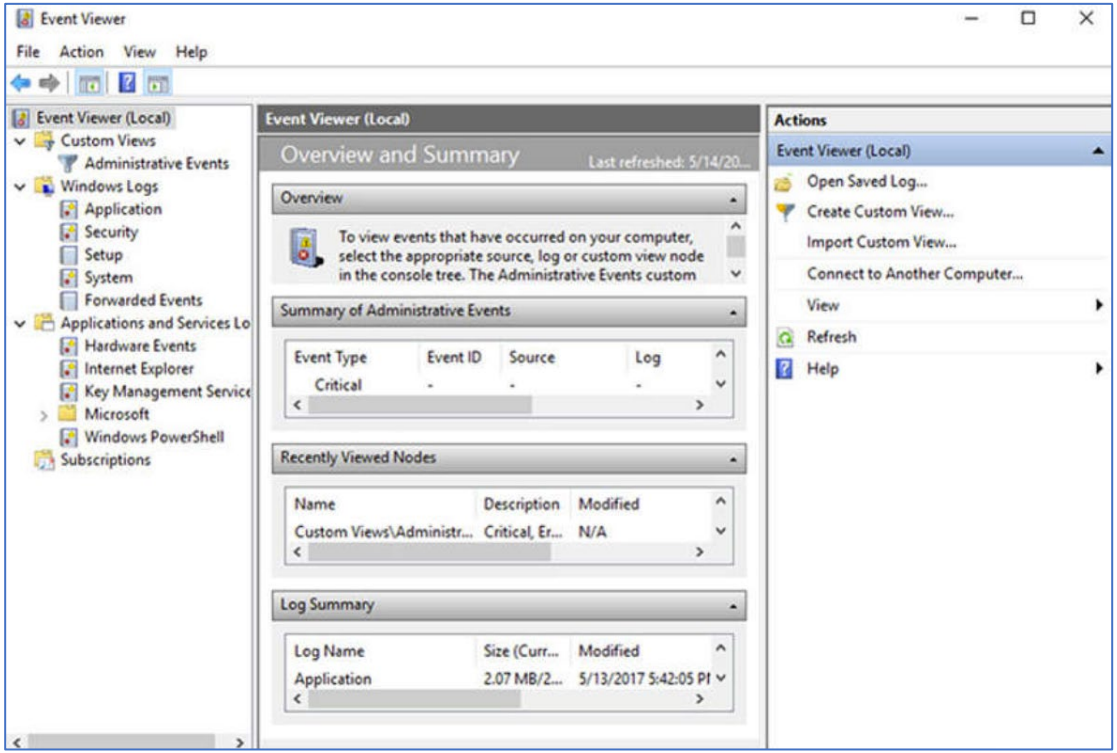
- To make this process easier, you can link the connections to the running processes that created them in Task Manager. To do this, open a command prompt with administrative privileges and enter the **netstat -abno** command, as shown in the command output in the next slide.

The netstat Command (Cont.)

```
Microsoft Windows [Version 10.0.18363.720]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\WINDOWS\system32> netstat -abno
Active Connections
  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       952
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    0.0.0.0:623            0.0.0.0:0              LISTENING       14660
 [LMS.exe]
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       1396
  TermService
 [svchost.exe]
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       9792
  CDPSvc
 [svchost.exe]
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    0.0.0.0:5593           0.0.0.0:0              LISTENING       4
```

- Examining the active TCP connections, an analyst should be able to determine if there are any suspicious programs listening for incoming connections on the host.
- The process can be traced to the Windows Task Manager and cancelled.
- If more than one process is listed with the same name, use the PID to find the correct process.
- To display the PIDs for the processes in the Task Manager, open the **Task Manager**, right-click the table heading and select **PID**.

Event Viewer



- Windows Event Viewer logs the history of application, security, and system events.
- These log files are a valuable troubleshooting tool because they provide information necessary to identify a problem.
- To open the Event Viewer, search for it and click the program icon, as shown in the figure.

Event Viewer (Cont.)

- Windows includes two categories of event logs:
  - Windows Logs
  - Application and Services Logs

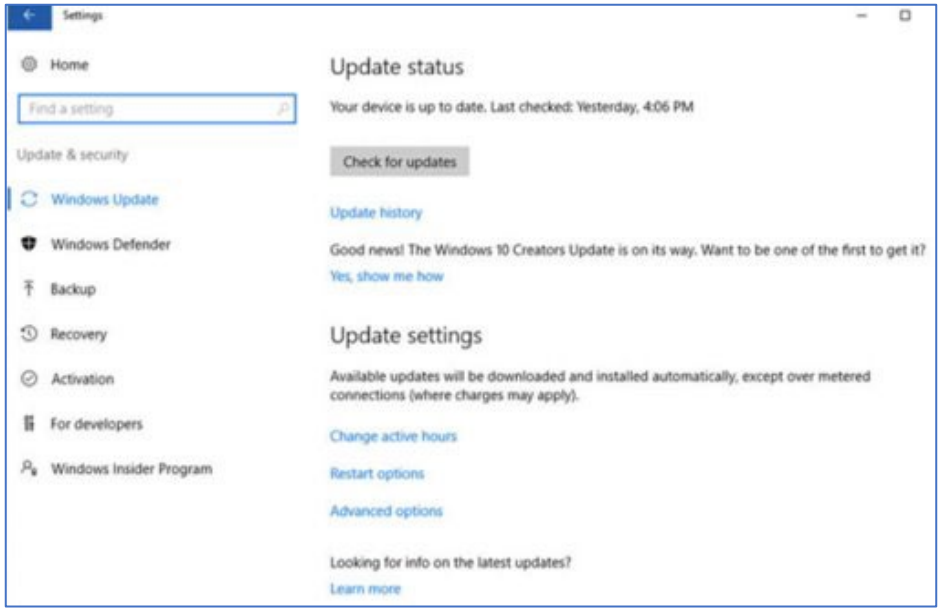
- Events that are displayed in these logs have data of:
  - level: information, warning, error, or critical
  - date and time that the event occurred
  - source of the event and an ID which relates to that type of event

- Security event logs are found under Windows Logs.
- They use event IDs to identify the type of event.

Windows Update Management

- Attackers are constantly producing new ways to compromise computers and exploit bad code.
- Microsoft is always trying to stay ahead of the attackers, so always make sure Windows is up to date with the latest service packs and security patches.
- Patches are code updates that manufacturers provide to prevent a newly discovered virus or worm from making a successful attack.

Windows Update Management (Cont.)



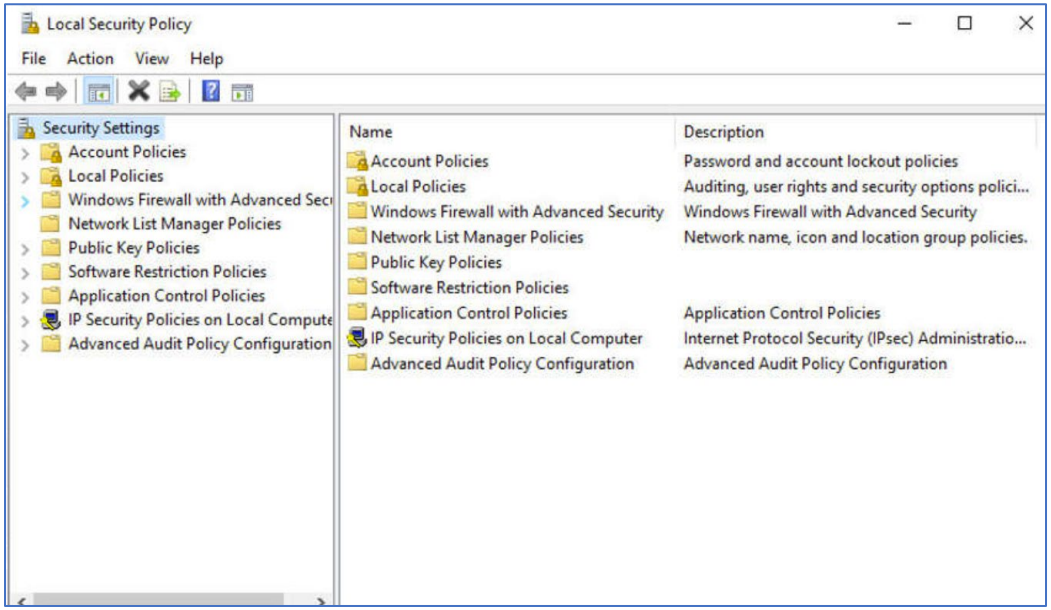
- Windows routinely checks the Windows Update website for high-priority updates that can help protect a computer from the latest security threats.
  - These updates include security updates, critical updates, and service packs.
  - Update status, shown in the figure, allows you to check for updates manually and see the update history of the computer.

Local Security Policy

- A security policy is a set of objectives that ensures the security of a network, the data, and the computer systems in an organization.

- The security policy is a constantly evolving document based on changes in technology, business, and employee requirements.

Local Security Policy (Cont.)



- Active Directory is configured with Domains on a Windows Server.
- The admin configures a Domain Security Policy that applies to all computers that join the domain.
- Account policies are automatically set when a user logs in to a computer that is a member of a domain.
- Windows Local Security Policy, **shown in the figure**, can be used for stand-alone computers that are not part of an Active Directory domain.

Local Security Policy (Cont.)

- Password guidelines are an important component of a security policy.
- Passwords help prevent theft of data and malicious acts.
- Use the Account Lockout Policy in Account Policies to prevent brute-force login attempts.
- A security policy should contain a rule about requiring a computer to lock when the screensaver starts.
- If the Local Security Policy on every stand-alone computer is the same, then use the Export Policy feature.
- The Local Security Policy applet contains many other security settings that apply specifically to the local computer.
    - You can configure User Rights, Firewall Rules, and even the ability to restrict the files that users or groups are allowed to run with the AppLocker.

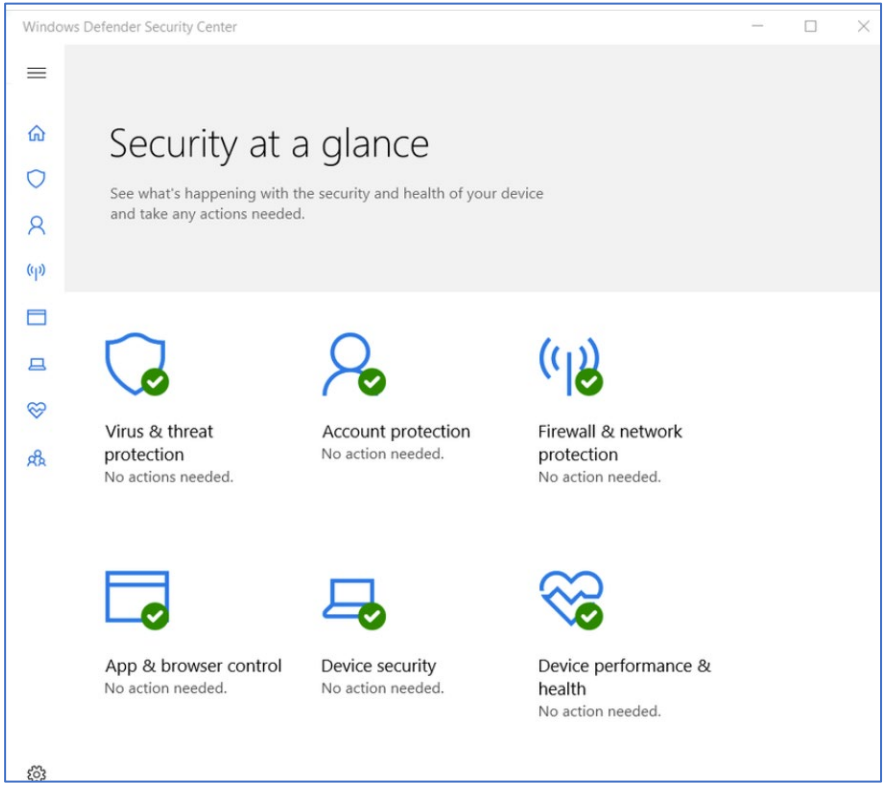
Windows Defender

Malware includes viruses, worms, Trojan horses, keyloggers, spyware, and adware. These are designed to invade privacy, steal information, damage the computer, or corrupt data. It is important that you protect computers and mobile devices using reputable antimalware software. The following types of antimalware programs are available:

Antimalware Programs	Description
Antivirus protection	This program continuously monitors for viruses. When a virus is detected, the user is warned, and the program attempts to quarantine or delete the virus.
Adware protection	This program continuously looks for programs that display advertising on your computer.
Phishing protection	This program blocks the IP addresses of known phishing websites and warns the user about suspicious sites.
Spyware protection	This program scans for keyloggers and other spyware.
Trusted/untrusted sources	This program warns you about unsafe programs about to be installed or unsafe websites before they are visited.

It may take several different programs and multiple scans to completely remove all malicious software. Run only one malware protection program at a time.

Windows Defender (Cont.)

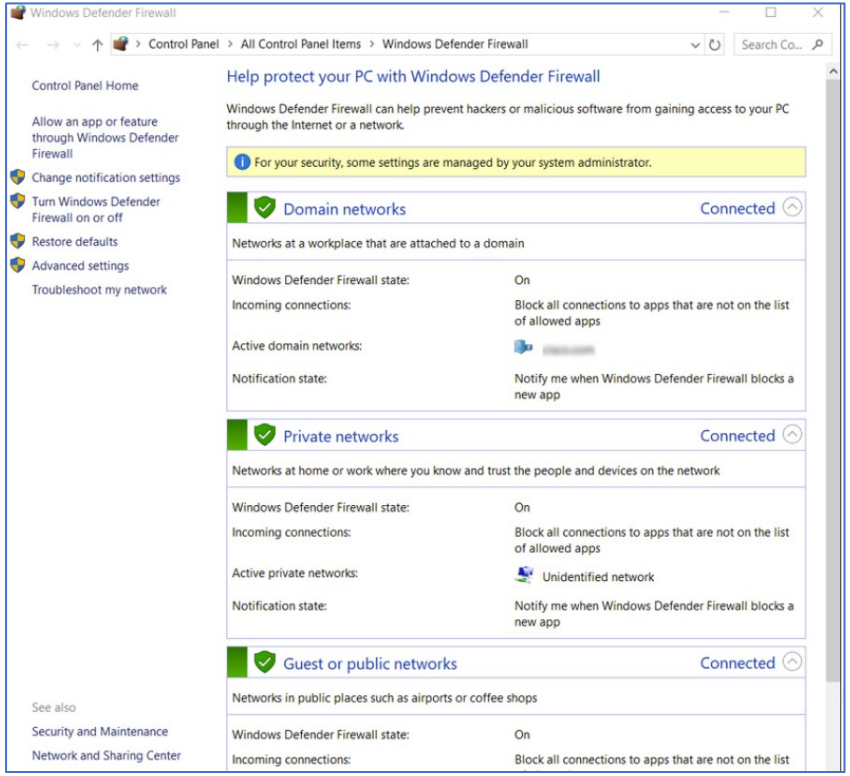


- Several reputable security organizations such as McAfee, Symantec, and Kaspersky offer all-inclusive malware protection for computers and mobile devices.
- Windows has built-in virus and spyware protection called Windows Defender, as shown in the figure.
- Windows Defender is turned on by default to provide real-time protection against infection.

Windows Defender Firewall

- A firewall selectively denies traffic to a computer or network segment.
- Firewalls generally work by opening and closing the ports used by various applications.
  - By opening only the required ports on a firewall, you are implementing a restrictive security policy.
  - Any packet not explicitly permitted is denied.

Windows Defender Firewall (Cont.)



- To allow program access through the Windows Defender Firewall, search for **Control Panels**. Under **Systems and Security**, locate **Windows Defender Firewall**. Click **Allow an app or feature through Windows Defender Firewall**, as shown in the figure.
- To use a different software firewall, you will need to disable Windows Firewall. To disable the Windows Firewall, click **Turn Windows Firewall on or off**.
- Many additional settings can be found under **Advanced settings**.

7.5 The Windows Operating System Summary

What Did I Learn in this Module?

Windows History:

- Microsoft developed MS-DOS as a command line interface (CLI) to access the disk drive and load the operating system files.
- Modern Windows versions are in direct control of the computer and its hardware and support multiple user processes.
- Users use a Windows GUI to work with data files and software.
    - The GUI has a main area that is known as the Desktop and a Task Bar situated below the desktop.
        - The Task Bar includes the Start menu, quick launch icons, and a notification area. Windows has many vulnerabilities.

What Did I Learn in this Module? (Cont.)

Windows Architecture and Operations:

- Windows consists of a hardware abstraction layer (HAL); software that handles the communication between the hardware and the kernel.
  - The kernel has control over the entire computer and handles input and output requests, memory, and the peripherals connected to the computer.
- Windows supports several different file systems, but NTFS is the most widely used.
  - NTFS volumes include the partition boot sector, master file table, system files and the file area.
- A computer works by storing instructions in RAM until the CPU processes them.
  - Each process in a 32-bit Windows computer supports a virtual address space that enables addressing up to 4 gigabytes.
  - Each process in a 64-bit Windows computer supports a virtual address space of up to 8 terabytes.

What Did I Learn in this Module? (Cont.)

Windows Configuration and Monitoring:

- For security, it is not advisable to log on to Windows using the admin account.
  - Do not give standard users administrative privileges.
  - Do not enable the Guests account.
- You can use the CLI or the Windows PowerShell to execute commands.
- PowerShell can be used to create scripts to automate tasks that the regular CLI is unable to automate.
- Windows Management Instrumentation (WMI) is used to manage remote computers.
- Task Manager provides a lot of information about what is running, and the general performance of the computer.
- The Resource Monitor provides more detailed information about resource usage.
- The Network and Sharing Center is used to configure Windows networking properties and test networking settings.
- The Server Message Block (SMB) protocol is used to share network resources such as files on remote hosts.
- The Universal Naming Convention (UNC) format is used to connect to resources.
- Windows Server is an edition of Windows that is mainly used in data centers.

What Did I Learn in this Module? (Cont.)

Windows Security:

- Malware can open communication ports to communicate and spread.
- The Windows netstat command displays all open communication ports on a computer and can also display the software processes that are associated with the ports.
  - This enables unknown potentially malicious software to be identified and shutdown.
- Windows Event Viewer provides access to numerous logged events regarding the operation of a computer.
- Windows logs Windows events and applications and services events.
  - Logged event severity levels range through the information, warning, error, or critical levels.