3.1 Windows History

3.1.1 Disk Operating System

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. DOS provides a file system which organizes the files in a specific way on the disk. Microsoft bought DOS and developed MS-DOS.

Early versions of Windows consisted of a Graphical User Interface (GUI) that ran over MS-DOS, starting with Windows 1.0 in 1985. The disk operating system still controlled the computer and its hardware. A modern operating system like Windows 10 is not considered a disk operating system. It is built on Windows NT, which stands for "New Technologies". The operating system itself is in direct control of the computer and its hardware. NT is an OS with support for multiple user processes.

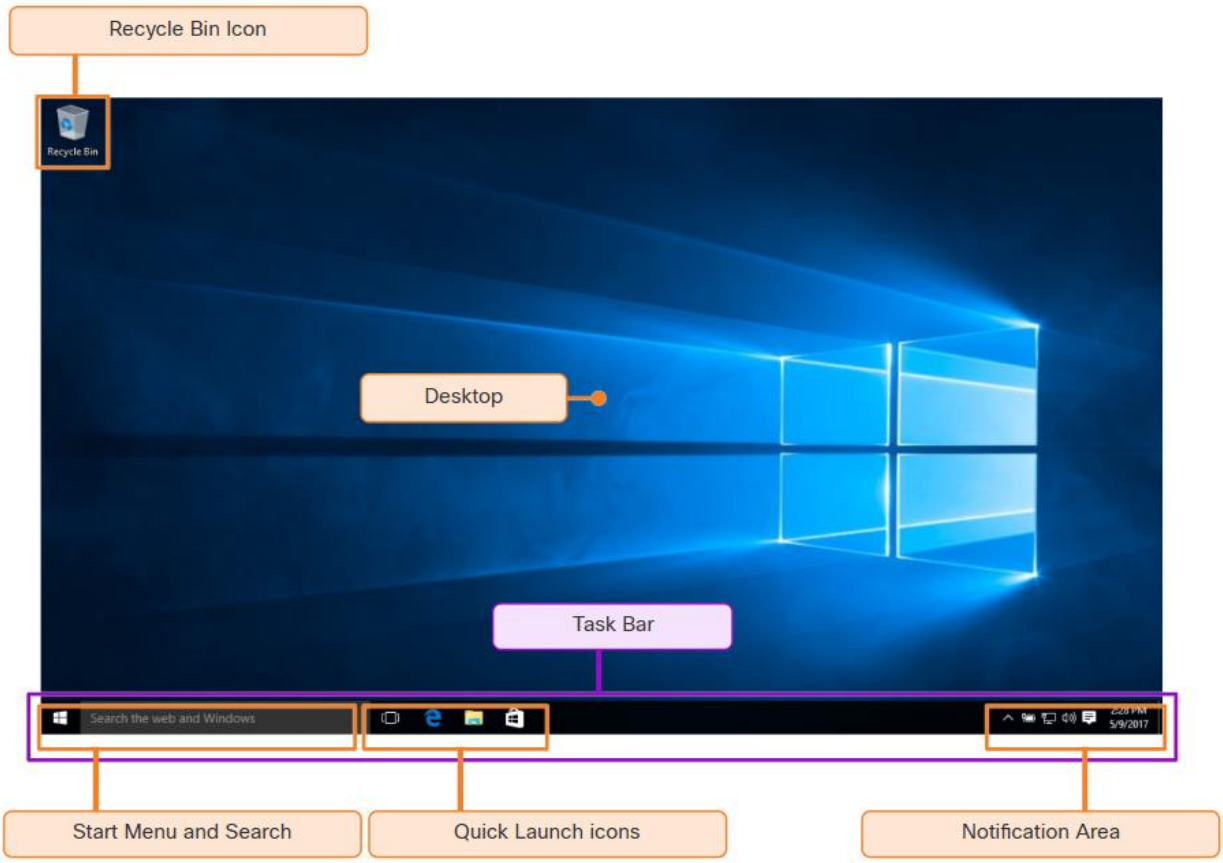
MS-DOS Command	Description
dir	Shows a listing of all the files in the current directory (folder)
cd *directory*	Changes the directory to the indicated directory
cd ..	Changes the directory to the directory above the current directory
**cd **	Changes the directory to the root directory (often C:)
copy *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

3.1.2 Windows Versions

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

3.1.3 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

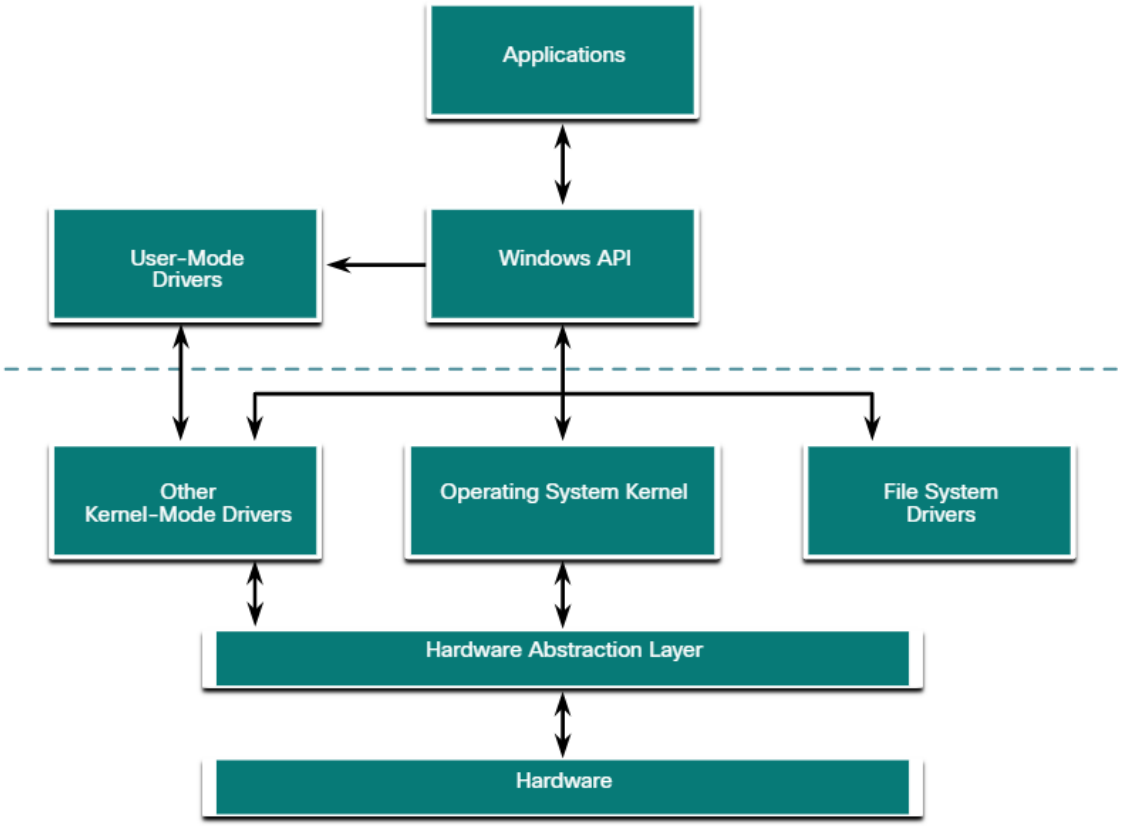

Recycle Bin Icon
Recycle Bin
Desktop
Task Bar
Search the web and Windows
Start Menu and Search
Quick Launch icons
Notification Area

3.1.4 Operating System Vulnerabilities

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.
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 that 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.

3.2 Windows Architecture and operators

3.2.1 Hardware Abstraction Layer



Basic Windows Architecture

A hardware abstraction layer HAL is a software that handles all the communication between hardware and the kernel.

3.2.2 User mode and kernel mode

CPU operates in two different modes when computer has windows installed .

- Installed application runs in user modes
- Operating system code runs in kernel mode

3.2.3 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.

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

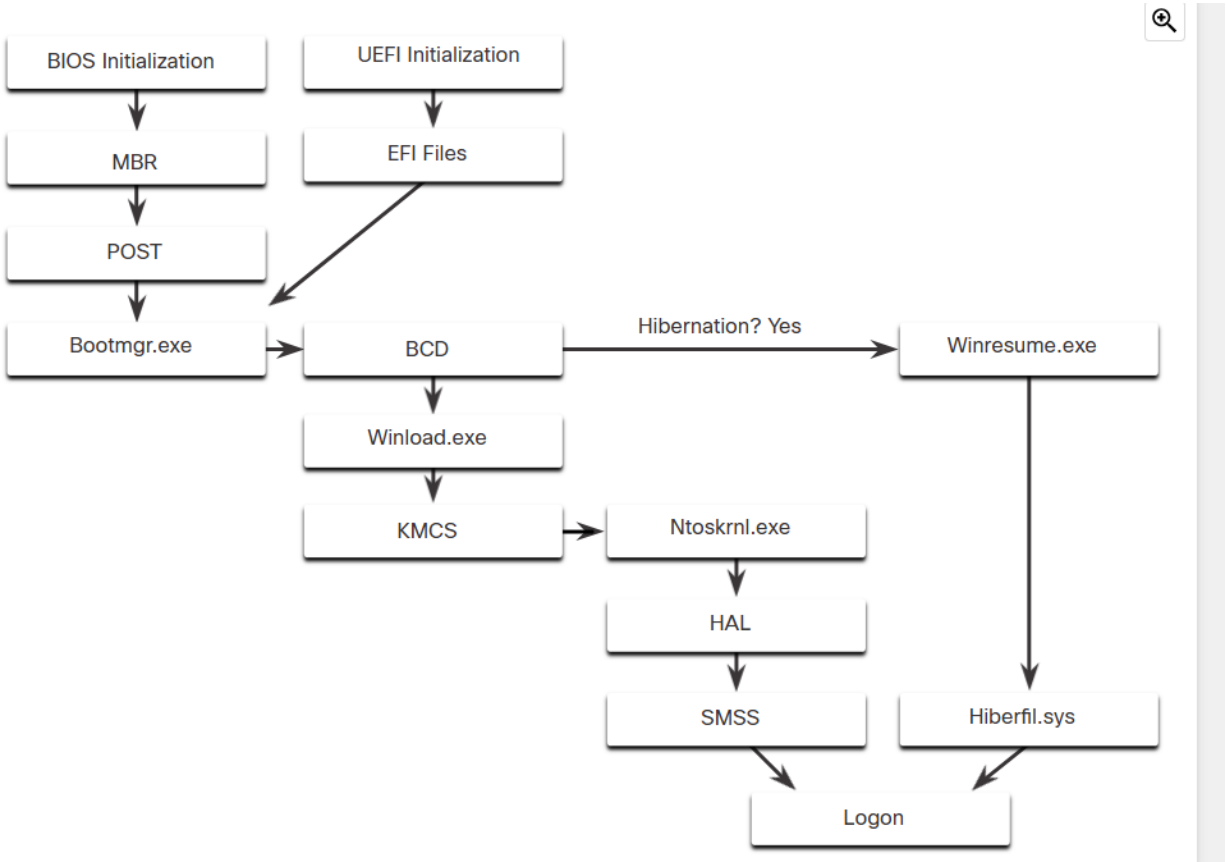
- Partition Boot Sector - This is the first 16 sectors of the drive. It contains the location of the Master File Table (MFT). The last 16 sectors contain a copy of the boot sector.
- Master File Table (MFT) - This table contains the locations of all the files and directories on the partition, including 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.

3.2.4 Alternate Data Streams (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. This is sometimes used by applications that are storing additional information about the file. The ADS is an important factor when discussing malware. This is because it is easy to hide data in an ADS. An attacker could store malicious code within an ADS that can then be called from a different file.

3.2.5 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.



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.

In BIOS firmware, 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 all of 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.

In contrast to BIOS firmware, UEFI firmware has a lot of visibility into the 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).

Whether the firmware is BIOS or UEFI, after a valid Windows installation is located, the **Bootmgr.exe** file is run. **Bootmgr.exe** switches the system from real mode to protected mode so that all of the system memory can be used.

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 all of the settings, options, hardware, and software the computer has. The registry will be explored in depth later in this chapter. **Winload.exe** also uses Kernel Mode Code Signing (KMCS) to make sure that all drivers are digitally signed. This ensures that the drivers are safe to load as the computer starts.

After the drivers have been examined, **Winload.exe** runs **Ntoskrnl.exe** which starts the Windows kernel and sets up the HAL. Finally, 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.

3.2.6 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.

3.2.7 Windows Shutdown

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

3.2.8 Process, 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.

All of the threads dedicated to a process are contained within the same address space. This means that these threads may not access the address space of any other process. This prevents corruption of other processes. Because Windows multitasks, multiple threads can be executed at the same time. The amount of threads that can be executed at the same time is dependent on the number of the computer's processors.

Some of the processes that Windows runs are services. These are programs that run in the background to support the operating system and applications. They can be set to start automatically when Windows boots or they can be started manually. They can also be stopped, restarted, or disabled.

Services provide long-running functionality, such as wireless or access to an FTP server. To configure Windows Services, search for services. The Windows Services control panel applet is shown in the figure.

3.2.9 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. The virtual address is not the actual physical location in memory, but an entry in a page table that is used to translate the virtual address into the physical address.

A powerful tool for viewing memory allocation is RAMMap.

3.2.10 The Windows Registry

Windows stores all of the information about hardware, applications, users, and system settings in a large database known as the registry.

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 registry keys and values in the hives can be created, modified, or deleted by an account with administrative privileges. The tool **regedit.exe** is used to modify the registry.

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

3.3 Windows Configuration and Monitoring

3.3.1 Run as Administrator

it is necessary to run or install software that requires the privileges of the Administrator.

3.3.2 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. This is known as a local user. This account will contain all of your customization settings, access permissions, file locations, and many other user-specific data. There are also two other accounts that are present, the guest, and the administrator. Both of these accounts are disabled by default.

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. A user can be placed into multiple groups to be provided with many different permissions. When the permissions overlap, certain permissions, like "explicitly deny" will override the permission provided by a different group.

Local users and groups are managed with the **lusrmgr.msc** control panel applet.

In addition to groups, Windows can also use domains to set permissions. A domain is a type of network service where all of the users, groups, computers, peripherals, and security settings are stored on and controlled by a database. This database is stored on special computers or groups of computers called domain controllers (DCs).

3.3.3 CLI and Power shell

The Windows command line interface (CLI) can be used to run programs, navigate the file system, and manage files and folders. In addition, files called batch files can be created to execute multiple commands in succession, much like a basic script. To open the Windows CLI, search for **cmd.exe** and click the program.

Another environment, called the Windows PowerShell, can be used to create scripts to automate tasks that the regular CLI is unable to create. PowerShell also provides a CLI for initiating commands. PowerShell is an integrated program within Windows and can be opened by searching for "powershell" and clicking the program. Like the CLI, PowerShell can also be run with administrative privileges.

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.

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

3.3.4 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**.

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

3.3.5 The net Command

Windows has many commands that can be entered at the command line. 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.

To see a list of the many **net** commands, type **net help** at the command prompt. The command output shows the commands that the **net** command can use. To see verbose help about any of the net commands, type C:> **net help**, as shown below.

3.3.6 Task Manager and Resource Monitor

Task Manager

The Task Manager provides a lot of information about the software that is running and the general performance of the computer.

Task Manager Tabs	Description
Processes	• Lists all of 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 of 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**.
Users	• All of 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.

Resource Monitor

When more detailed information about resource usage is needed, you can use the Resource Monitor.

Resource Monitor Tabs	Description
Overview	• The tab displays the general usage for each resource. • If you select a single process, it will be filtered across all of the tabs to show only that process's statistics.
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 of 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 of 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 of 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.

3.3.7 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. The easiest way to run this tool is to search for it and click it. Use the Network and Sharing Center to verify or create network connections, configure network sharing, and change network adapter settings.

Network and Sharing Center

The initial view shows an overview of the active network. This view shows whether there is internet access and if the network is private, public, or guest. The type of network, either wired or wireless, is also shown. From this window, you can see the HomeGroup the computer belongs to, or create one if it is not already part of a HomeGroup. This tool can also be used to change adapter settings, change advance sharing settings, set up a new connection, or troubleshoot problems. Note that HomeGroup was removed from Windows 10 in version 1803.

Change Adapter Settings

To configure a network adapter, choose **Change adapter settings** in the Networking and Sharing Center to show all of the network connections that are available. Select the adapter that you want to configure.

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 websitename** at the command prompt to find the address of the website webserver. When the address is returned, you know that DNS is functioning correctly. You can also check to see what ports are open, where they are connected, and what their current status is. Type **netstat** at the command line to see details of active network connections.

3.3.8 Accessing Network Resources

Like other operating systems, Windows uses networking for many different applications such as web, email, and file services. Originally developed by IBM, 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

In the UNC, servername is the server that is hosting the resource. This can be a DNS name, a NetBIOS name, or simply an IP address. The sharename is the root of the folder in the file system on the remote host, while the file is the resource that the local host is trying to find. The file may be deeper within the file system and this hierarchy will need to be indicated

Besides accessing shares on remote hosts, you can also log in to a remote host and manipulate that computer, as if it were local, to make configuration changes, install software, or troubleshoot an issue. In Windows, this feature uses the Remote Desktop Protocol (RDP).

3.3.9 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.

Note: Although there is a Windows Server 2000, it is considered a client version of Windows NT 5.0. Windows Server 2003 is a server based on NT 5.2 and begins a new family of Windows Server versions.

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

3.4 Windows Security

3.4.1 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 of the active TCP connections. 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.

```
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
Can not obtain ownership information
  TCP    0.0.0.0:8099           0.0.0.0:0              LISTENING       5248
[SolarWinds TFTP Server.exe]
  TCP    0.0.0.0:16992          0.0.0.0:0              LISTENING       14660
```

3.4.2 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.

Windows includes two categories of event logs: Windows Logs, and Application and Services Logs. Each of these categories has multiple log types. Events that are displayed in these logs have a level: information, warning, error, or critical. They also have the date and time that the event occurred, along with the source of the event and an ID which relates to that type of event.

There is a built-in custom view called Administrative Events that shows all critical, error, and warning events from all of the administrative logs. This is a good view to start with when trying to troubleshoot a problem.

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

3.4.3 Windows Update Management

No software is perfect, and the Windows operating system is no exception. Attackers are constantly coming up with new ways to compromise computers and exploit bad code. Some of these attacks come so quickly that defenses against them have not yet been devised and distributed. These are called zero-day exploits. Microsoft and security software developers are always trying to stay ahead of the attackers, but they are not always successful. To ensure the highest level of protection against these attacks, 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.

3.4.4 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.

In most networks that use Windows computers, Active Directory is configured with Domains on a Windows Server. Windows computers join the domain. The administrator 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.

3.4.5 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:

- 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.

3.4.6 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. In contrast, a permissive security policy permits access through all ports, except those explicitly denied. 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.

If you wish 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**.