02 Windows OS

Notebook:	FGA Cyber		
Created:	7/3/2019 9:22 AM	**Updated:**	7/3/2019 10:01 PM
Author:	clink200032@gmail.com		
URL:	https://static-course-assets.s3.amazonaws.com/CyberOps11/en/course/module2/2.1.1.4...		

2.1 Windows Overview
2.1.1 History

Windows XP = First 64 bit edition avaliable -> can address 16,8 TB RAM

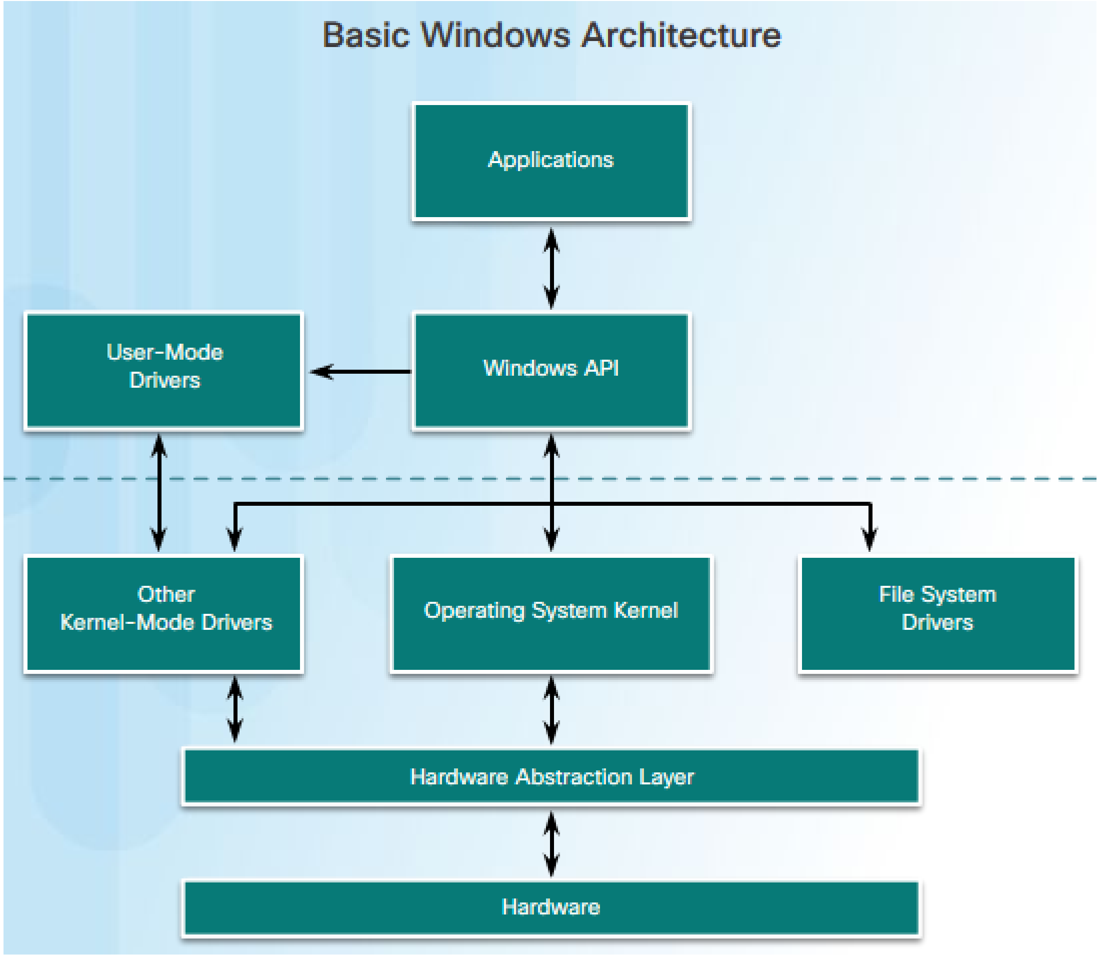
OS Vulnerability

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 manipulate data.

These are some common Windows OS Security Recommendations:

- **Virus or malware protection** – By default, Windows uses Windows Defender. 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.

2.1.2 Windows Architecture and Operation



Windows computers use many different types of hardware. The operating system can be installed on a computer off of the shelf, or a computer built from the ground up. When the operating system is installed, it must be isolated from differences in hardware. The basic Windows architecture is shown in the figure. A hardware abstraction layer (HAL) is code that handles all of 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 of the input and output requests, memory, and all of the 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

There are two different modes in which a CPU operates when the computer has Windows installed: the user mode and the kernel mode. 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 is capable of executing any CPU instruction. Kernel mode code also can reference any memory address directly. Generally reserved for the most trusted functions of the OS, crashes in code running in kernel mode stop the operation of the entire computer. Conversely, programs such as user applications, run in user mode and have no direct access to hardware or memory locations. User mode code must go through the operating system to access hardware resources. Because of the isolation provided by user mode, crashes in user mode are restricted to the application only and are recoverable. Most of the programs in Windows run in user mode. Device drivers, pieces of software that allow the operating system and a device to communicate, may run in either kernel or user mode, depending on the driver.

All of the code that runs in kernel mode uses the same address space. Kernel-mode drivers have no isolation from the operating system. If an error occurs with the driver running in kernel mode, and it writes to the wrong address space, the operating system or another kernel-mode driver could be adversely affected. In this respect, the driver might crash, causing the entire operating system to crash.

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. By having its own process, that application has its own private address space, rendering other applications unable to modify the data in it. This also helps to prevent the operating system and other applications from crashing if that application crashes.

Windows File System

A file system is how information is organized on storage media. Some file systems may be a better choice to use than others, depending on the type of media that will be used. These are the file systems that Windows supports:

- **File Allocation Table (FAT)** – 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.
- **exFAT** – This is an extended version of FAT that has even fewer restrictions than FAT32, but is not supported very well outside of the Windows ecosystem.
- **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 while Mac-OS X computers can only read an NTFS partition. They are able to write to an NTFS partition after installing special drivers.

NTFS is the most widely used file system for Windows for many reasons. NTFS supports very large files and partitions; it is very compatible with other operating systems. NTFS is also very reliable and supports recovery features. Most importantly, it supports many security features. Data access control is achieved through security descriptors. These security descriptors contain file ownership and permissions all the way down to the file level. NTFS also tracks many time stamps to track file activity. Sometimes referred to as MACE, the timestamps Modify, Access, Create, and Entry Modified are often used in forensic investigations to determine the history of a file or folder. NTFS also supports file system encryption to secure the entire storage media.

Alternate Data Streams

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.

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

- The first command places the text “Alternate Data Here” into an ADS of the file Testfile.txt called “ADS”.
- The next command, **dir**, shows that the file was created, but the ADS is not visible.
- The next command shows that there is data in the Testfile.txt:ADS data stream.
- The last command shows the ADS of the Testfile.txt file because the **r** switch was used with the **dir** command.

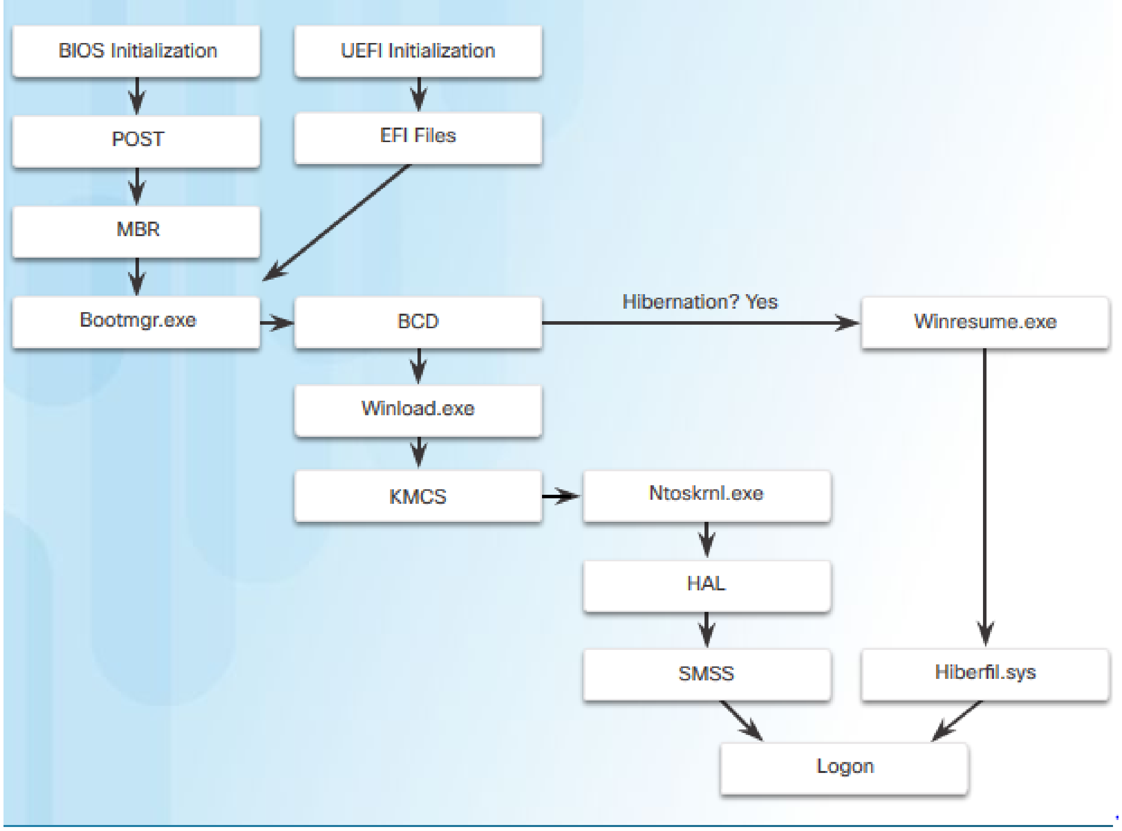
Before a storage device such as a disk can be used, it must be formatted with a file system. In turn, before a file system can be put into place on a storage device, the device needs to be partitioned. A hard drive is divided into areas called partitions. Each partition is a logical storage unit that can be formatted to store information, such as data files or applications. During the installation process, most operating systems automatically partition and format the available drive space with a file system such as NTFS.

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.
- **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.

Windows boot process



Many actions occur between the time when the computer power button is pressed and Windows is fully loaded, as shown in the figure.

Two types of computer firmware exist: Basic Input-Output System (BIOS) and Unified Extended Firmware Interface (UEFI). 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. 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).

Note: A computer that uses UEFI stores boot code in the firmware. This helps to increase the security of the computer at boot time because the computer goes directly into protected mode.

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.

Windows Startup and Shutdown

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. These entries can be manually entered into the registry, but it is much safer to use the Msconfig.exe tool. This tool is used to view and change all of the start-up options for the computer. Use the search box to find and open the Msconfig tool.

There are five tabs which contain the configuration options:

• **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. The General tab is shown in Figure 1.

• **Boot** – Any installed operating system can be chosen here to start. There are also options for Safe boot, which is used to troubleshoot startup. The Boot tab is shown in Figure 2.

• **Services** – All the installed services are listed here so that they can be chosen to start at startup. The Services tab is shown in Figure 3

• **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. The Startup tab is shown in Figure 4.

• **Tools** – Many common operating system tools can be launched directly from this tab. The Tools tab is shown in Figure 5.

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. The computer needs time to close each application, shut down each service, and record any configuration changes before power is lost.

During shutdown, the computer will close user mode applications first, followed by kernel mode processes. If a user mode process does not respond within a certain amount of time, the OS will display notification and allow the user to wait for the application to respond, or forcibly end the process. If a kernel mode process does not respond, the shutdown will appear to hang, and it may be necessary to shut down the computer with the power button.

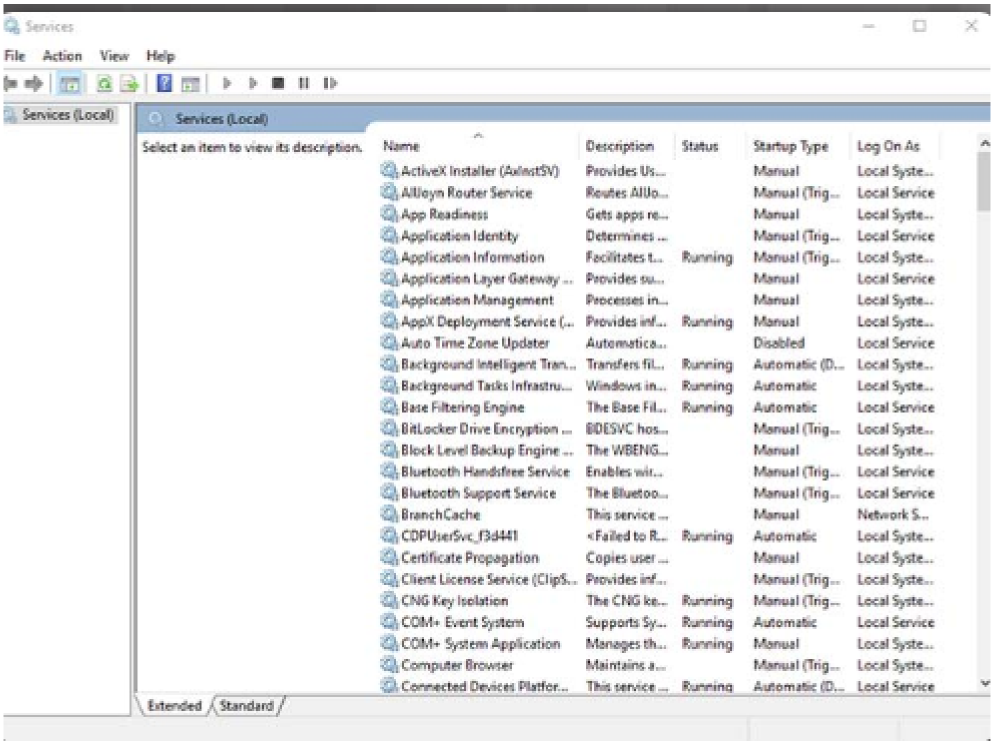
There are several ways to shut down a Windows computer: Start menu power options, the command line command **shutdown**, and using **Ctrl+Alt+Delete** and clicking the power icon. There are three different options from which to choose when shutting down the computer: Shutdown, which turns the computer off, Restart, which re-boots the computer from scratch, and Hibernate which 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.

Process Thread and service

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 Figure 1.

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.

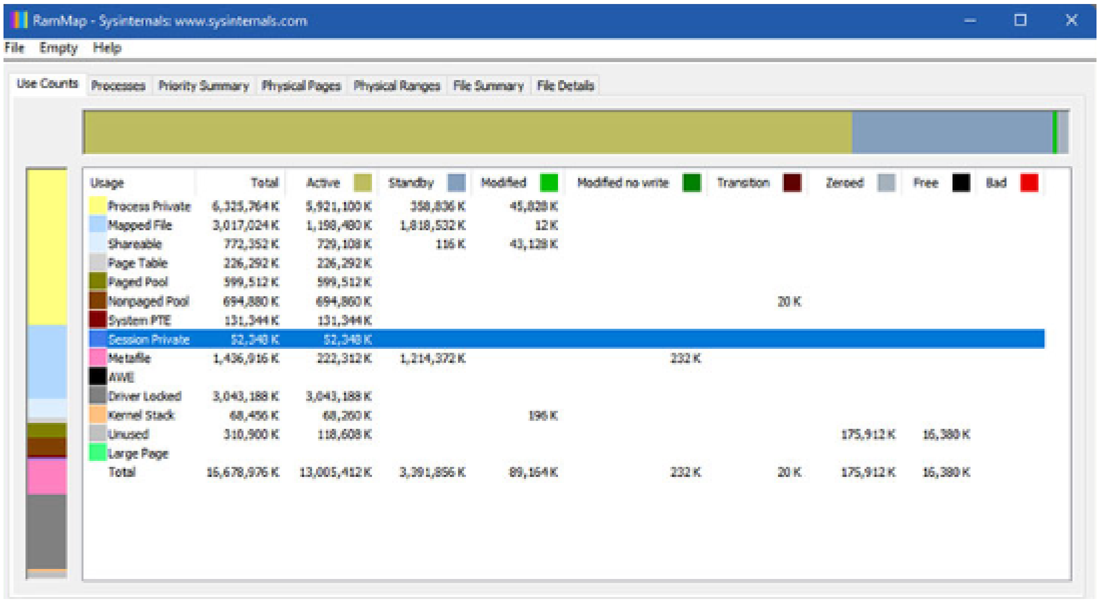
Some of the processes that Windows runs are services. **These are programs that run in the background to support the operating system and applications**. They can be set to start automatically when Windows boots or they can be started manually. They can also be stopped, restarted, or disabled. Services 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 Figure 2. Be very careful when manipulating the setting of these services. Some programs rely on one or more services to operate properly. Shutting down a service may adversely affect applications, or other services.



Select an item to view its description.

Name	Description	Status	Startup Type	Log On As
ActiveX Installer (AxInstSV)	Provides Us...		Manual	Local Syste...
AllJoyn Router Service	Routes AllJo...		Manual (Trig...	Local Service
App Readiness	Gets apps re...		Manual	Local Syste...
Application Identity	Determines ...		Manual (Trig...	Local Service
Application Information	Facilitates t...	Running	Manual (Trig...	Local Syste...
Application Layer Gateway ...	Provides su...		Manual	Local Service
Application Management	Processes in...		Manual	Local Syste...
AppX Deployment Service (...	Provides inf...	Running	Manual	Local Syste...
Auto Time Zone Updater	Automatica...		Disabled	Local Service
Background Intelligent Tran...	Transfers fil...	Running	Automatic (D...	Local Syste...
Background Tasks Infrastru...	Windows in...	Running	Automatic	Local Syste...
Base Filtering Engine	The Base Fil...	Running	Automatic	Local Service
BitLocker Drive Encryption ...	BDESVC hos...		Manual (Trig...	Local Syste...
Block Level Backup Engine ...	The WBENG...		Manual	Local Syste...
Bluetooth Handsfree Service	Enables wir...		Manual (Trig...	Local Service
Bluetooth Support Service	The Bluetoo...		Manual (Trig...	Local Service
BranchCache	This service ...		Manual	Network S...
CDPUserSvc_f3d441	<Failed to R...	Running	Automatic	Local Syste...
Certificate Propagation	Copies user ...		Manual	Local Syste...
Client License Service (ClipS...	Provides inf...		Manual (Trig...	Local Syste...
CNG Key Isolation	The CNG ke...	Running	Manual (Trig...	Local Syste...
COM+ Event System	Supports Sy...	Running	Automatic	Local Service
COM+ System Application	Manages th...	Running	Manual	Local Syste...
Computer Browser	Maintains a...		Manual (Trig...	Local Syste...
Connected Devices Platfor...	This service ...	Running	Automatic (D...	Local Service

Memory Allocation and Handles



Usage	Total	Active	Standby	Modified	Modified no write	Transition	Zeroed	Free	Bad
Process Private	6,325,764 K	5,921,100 K	358,836 K	45,828 K					
Mapped File	3,017,024 K	1,198,480 K	1,818,532 K	12 K					
Shareable	772,352 K	729,108 K	116 K	43,128 K					
Page Table	226,292 K	226,292 K							
Paged Pool	599,512 K	599,512 K							
Nonpaged Pool	694,880 K	694,860 K				20 K			
System PTE	131,344 K	131,344 K							
Session Private	52,340 K	52,340 K							
Metafile	1,436,916 K	222,312 K	1,214,372 K		232 K				
AWE									
Driver Locked	3,043,188 K	3,043,188 K							
Kernel Stack	68,456 K	68,260 K		196 K					
Unused	310,900 K	118,608 K					175,912 K	16,380 K	
Large Page									
Total	16,678,976 K	13,005,412 K	3,391,856 K	89,164 K	232 K	20 K	175,912 K	16,380 K	

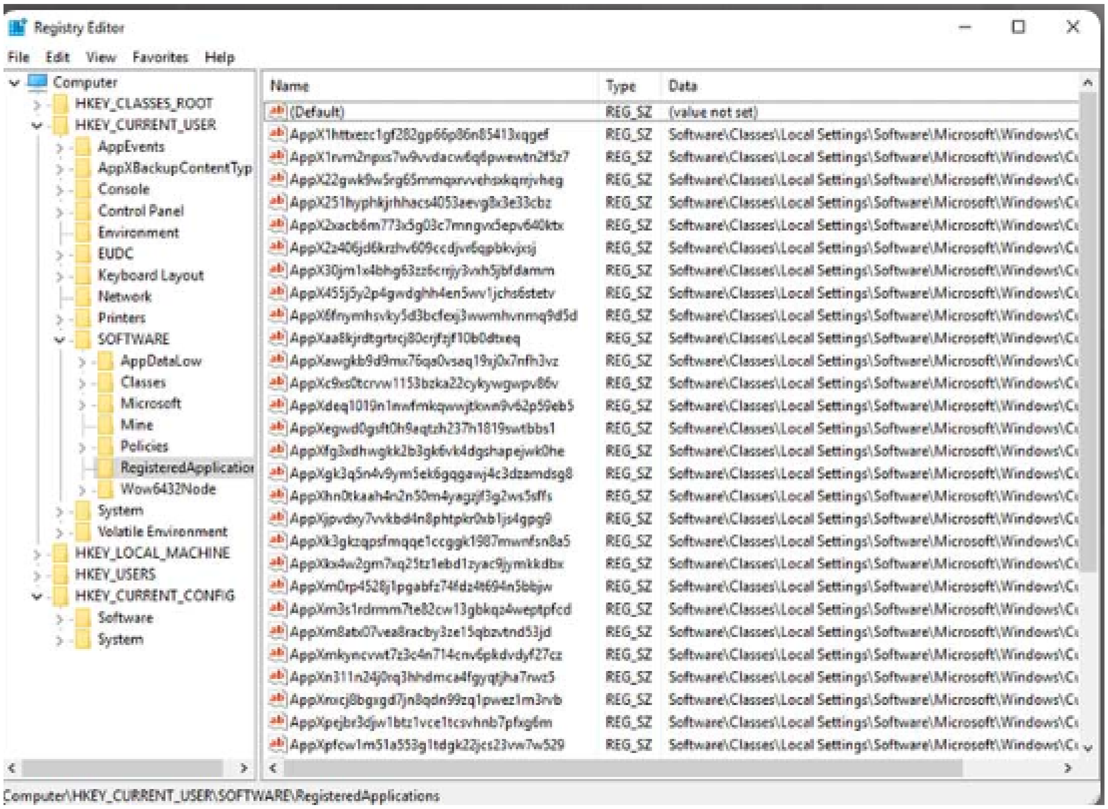
A computer works by storing instructions in RAM until the CPU processes them. The virtual address space for a process is the set of virtual addresses that the process can use. The virtual address is not the actual physical location in memory, but an entry in a page table that is used to translate the virtual address into the physical address.

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. This is because the user space process is not allowed to directly access these kernel resources. The process handle provides the access needed by the user space process without a direct connection to it.

One of the more powerful tools to view memory allocation is Sysinternal's RamMap, shown in the figure. Click here to download and learn more about RamMap.

Windows Registry



Name	Type	Data
(Default)	REG_SZ	(value not set)
AppX1hhtxezc1gf282gp66p86n85413xqgef	REG_SZ	Software\Classes\Local Settings\Software\Microsoft\Windows\C
AppX1rvm2npxs7w9vvdacw6q6pwewtn2f5z7	REG_SZ	Software\Classes\Local Settings\Software\Microsoft\Windows\C
AppX22gwk9w5rg65mmqxrvvehxkqrjvheg	REG_SZ	Software\Classes\Local Settings\Software\Microsoft\Windows\C
AppX251hyphkjrhhacs4053aevg8x3e33cbz	REG_SZ	Software\Classes\Local Settings\Software\Microsoft\Windows\C
AppX2xacb6m773x5g03c7mngvx5epv640ktx	REG_SZ	Software\Classes\Local Settings\Software\Microsoft\Windows\C
AppX2z406jd6krzhv609ccdjvr6qpbkvjxsj	REG_SZ	Software\Classes\Local Settings\Software\Microsoft\Windows\C
AppX30jm1x4bhg63zz6crjjy3vxh5jbfdamm	REG_SZ	Software\Classes\Local Settings\Software\Microsoft\Windows\C
AppX455j5y2p4gwdghh4en5wv1jchs6stetv	REG_SZ	Software\Classes\Local Settings\Software\Microsoft\Windows\C
AppX6fnymhsvky5d3bcfexj3wwmhvnmq9d5d	REG_SZ	Software\Classes\Local Settings\Software\Microsoft\Windows\C
AppXaa8kjrdtgrtrcj80crjfzjf10b0dtxeq	REG_SZ	Software\Classes\Local Settings\Software\Microsoft\Windows\C
AppXewgkb9d9mx76qa0vseq19xj0x7nfh3vz	REG_SZ	Software\Classes\Local Settings\Software\Microsoft\Windows\C
AppXc9xs0tcrvw1153bzka22cykywgwpv86v	REG_SZ	Software\Classes\Local Settings\Software\Microsoft\Windows\C
AppXdeq1019n1mwfmkqwwjtkwn9v62p59eb5	REG_SZ	Software\Classes\Local Settings\Software\Microsoft\Windows\C
AppXegwd0gsft0h9eqtzh237h1819swtbbs1	REG_SZ	Software\Classes\Local Settings\Software\Microsoft\Windows\C
AppXfg3xdhwgkk2b3gk6vk4dgshapejwk0he	REG_SZ	Software\Classes\Local Settings\Software\Microsoft\Windows\C
AppXgk3q5n4v9ym5ek6gqgawj4c3dzamdsg8	REG_SZ	Software\Classes\Local Settings\Software\Microsoft\Windows\C
AppXhn0tkaah4n2n50m4yagzjf3g2ws5sffs	REG_SZ	Software\Classes\Local Settings\Software\Microsoft\Windows\C
AppXjpvdxy7vvkbd4n8phtpkr0xb1js4gpg9	REG_SZ	Software\Classes\Local Settings\Software\Microsoft\Windows\C
AppXk3gkzqpsfmqqe1ccggk1987mwnfsn8a5	REG_SZ	Software\Classes\Local Settings\Software\Microsoft\Windows\C
AppXkx4w2gm7xq25tz1ebd1zyac9jymkkdbx	REG_SZ	Software\Classes\Local Settings\Software\Microsoft\Windows\C
AppXm0rp4528j1pgabfz74fdz4t694n5bbjw	REG_SZ	Software\Classes\Local Settings\Software\Microsoft\Windows\C
AppXm3s1rdmmm7te82cw13gbkqz4weptpfcd	REG_SZ	Software\Classes\Local Settings\Software\Microsoft\Windows\C
AppXm8atx07vea8racby3ze15qbzvtnd53jd	REG_SZ	Software\Classes\Local Settings\Software\Microsoft\Windows\C
AppXmkyncvwt7z3c4n714cnv6pkdvdyf27cz	REG_SZ	Software\Classes\Local Settings\Software\Microsoft\Windows\C
AppXn311n24j0rq3hhdmca4fgyqtjha7rwz5	REG_SZ	Software\Classes\Local Settings\Software\Microsoft\Windows\C
AppXroxcj8bgxgd7jn8qdn99zq1pwez1m3rvb	REG_SZ	Software\Classes\Local Settings\Software\Microsoft\Windows\C
AppXpejbr3djw1btz1vce1tcsvhnb7pfxg6m	REG_SZ	Software\Classes\Local Settings\Software\Microsoft\Windows\C
AppXpfcw1m51a553g1tdgk22jcs23vw7w529	REG_SZ	Software\Classes\Local Settings\Software\Microsoft\Windows\C

Computer\HKEY_CURRENT_USER\SOFTWARE\RegisteredApplications

Windows stores all of 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 all of 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, that store data, are stored in keys and subkeys. The registry key can be up to 512 levels deep.

These are the five hives of the Windows registry:

- **HKEY_CURRENT_USER (HKCU)** - Holds data concerning the currently logged in user.
- **HKEY_USERS (HKU)** - Holds data concerning all the user accounts on the host.
- **HKEY_CLASSES_ROOT (HKCR)** - Holds data about object linking and embedding (OLE) registrations.
- **HKEY_LOCAL_MACHINE (HKLM)** - Holds system-related data.
- **HKEY_CURRENT_CONFIG (HKCC)** - Holds data about the current hardware profile.

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.

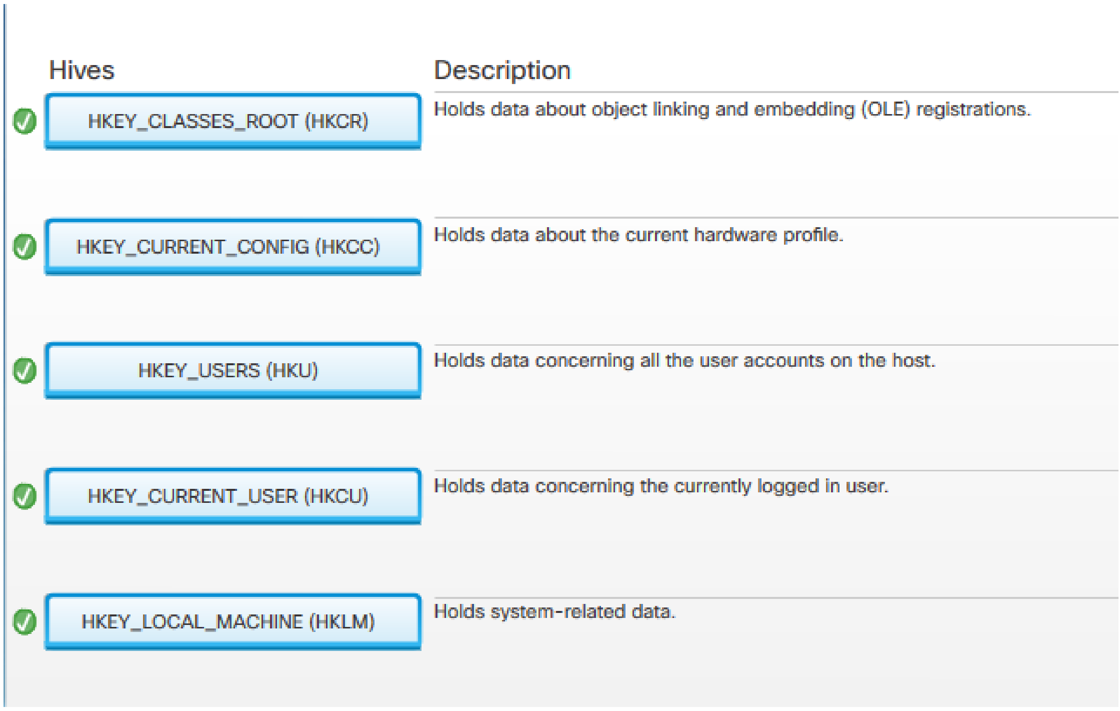
Navigation in the registry is very similar to Windows file explorer. Use the left panel to navigate the hives and the structure below it, and use the right panel to see the contents of the highlighted item in the left panel. With so many keys and subkeys, the key path can become very long. The path is displayed at the bottom of the window for reference. Because each key and subkey is essentially a container, the path is represented much like a folder in a file system. The backslash (\) is used to differentiate the hierarchy of the database.

Registry keys can contain either a subkey or a value. These are the different values that keys can contain:

- **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. During a normal boot, the user will not see the program start because the entry is in the registry and the application displays no windows or indication of starting when the computer boots. A keylogger, for example, would be devastating to the security of a computer if it were to start at boot without the user's knowledge or consent. When performing normal security audits, or remediating an infected system, review the application startup locations within the registry to ensure that each item is known and safe to run.

The registry also contains the activity that a user performs during normal day-to-day computer use. This includes the history of hardware devices, including all devices that have been connected to the computer including the name, manufacturer and serial number. Other information, such as what documents a user and program have opened, where they are located, and when they were accessed is stored in the registry. This is all very useful information when a forensics investigation needs to be performed.



	Hives	Description
✓	HKEY_CLASSES_ROOT (HKCR)	Holds data about object linking and embedding (OLE) registrations.
✓	HKEY_CURRENT_CONFIG (HKCC)	Holds data about the current hardware profile.
✓	HKEY_USERS (HKU)	Holds data concerning all the user accounts on the host.
✓	HKEY_CURRENT_USER (HKCU)	Holds data concerning the currently logged in user.
✓	HKEY_LOCAL_MACHINE (HKLM)	Holds system-related data.

2.2 WINDOWS ADMINISTRATION

2.2.1 Windows Config and Monitoring

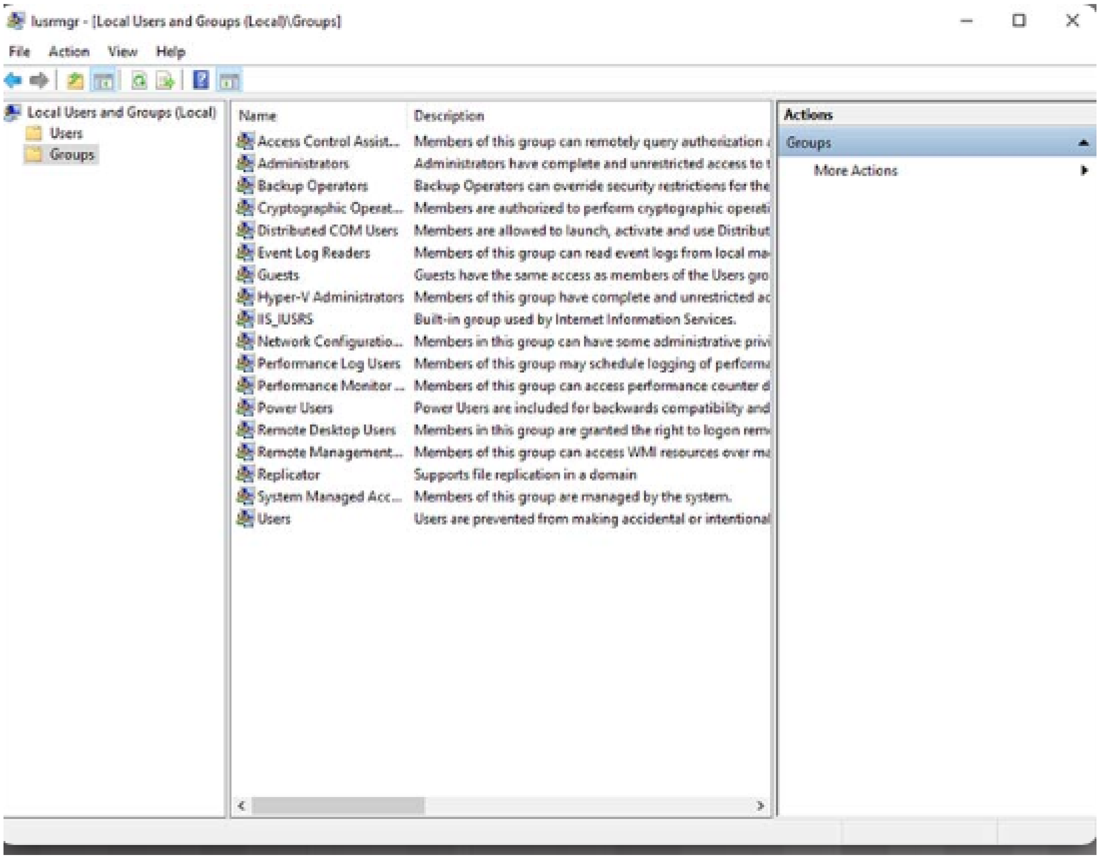
Run as Admin

As a security best practice, it is not advisable to log on to Windows using the Administrator account or an account with administrative privileges. This is because any program that is executed while logged on with those privileges will inherit them. Malware that has administrative privileges has full access to all the files and folders on the computer.

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:

- **Run as Administrator** – Right-click the command in the Windows File Explorer and choose **Run as Administrator** from the Context Menu, shown in Figure 1.
- **Administrator Command Prompt** – Search for **command**, right-click the executable file, and choose **Run as Administrator** from the Context Menu, shown in Figure 2. Every command that is executed from this command line will be carried out with the Administrator privileges, including installation of software.

Local user and Domains (lusrmgr.src)


lusrmgr - [Local Users and Groups (Local)\Groups]
File
Action
View
Help
Local Users and Groups (Local)
Users
Groups
Actions
Groups
More Actions

Name	Description
Access Control Assist...	Members of this group can remotely query authorization a
Administrators	Administrators have complete and unrestricted access to t
Backup Operators	Backup Operators can override security restrictions for the
Cryptographic Operat...	Members are authorized to perform cryptographic operati
Distributed COM Users	Members are allowed to launch, activate and use Distribut
Event Log Readers	Members of this group can read event logs from local ma
Guests	Guests have the same access as members of the Users gro
Hyper-V Administrators	Members of this group have complete and unrestricted ac
IIS_IUSRS	Built-in group used by Internet Information Services.
Network Configuratio...	Members in this group can have some administrative privi
Performance Log Users	Members of this group may schedule logging of performa
Performance Monitor ...	Members of this group can access performance counter d
Power Users	Power Users are included for backwards compatibility and
Remote Desktop Users	Members in this group are granted the right to logon rem
Remote Management...	Members of this group can access WMI resources over ma
Replicator	Supports file replication in a domain
System Managed Acc...	Members of this group are managed by the system.
Users	Users are prevented from making accidental or intentional

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.**

As a security best practice, do not enable the Administrator account and do not give standard users administrative privileges. If a user needs to perform any function that requires administrative privileges, the system will ask for the Administrator password and allow only that task to be performed as an administrator. By entering the administrator password, this protects the computer by preventing any software that is not authorized, from installing, executing, or accessing files.

The Guests account should not be enabled. The guest account does not have a password associated with it because it is created when a computer is going to be used by many different people who do not have accounts on the computer. Each time the guest account logs on, a default environment is provided to them with limited privileges.

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. There are many different user groups built in to Windows that are used for specific tasks. For example, the Performance Log Users group allows members to schedule logging of performance counters and collect logs either locally or remotely. Local users and groups are managed with the lusrmgr.msc control panel applet, as shown in the figure.

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)**. Each user and computer on the domain must authenticate against the DC to logon and access network resources. The security settings for each user and each computer are set by the DC for each session. Any setting supplied by the DC defaults to the local computer or user account setting.

PowerShell

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. Remember that right-clicking the program provides the option to Run as administrator, giving much more power to the commands that will be used.

The prompt displays the current location within the file system. These are a few things to remember when using the CLI:

- The file names and paths are not case-sensitive, by default.
- Storage devices are assigned a letter for reference. The letter, followed by a backslash (\) indicates the root of the device. Folder and file hierarchy on the device is indicated by separating them with the backslash. For example, C:\Users\Jim\Desktop\file.txt is the file called file.txt in the Desktop folder within the Jim folder within the Users folder on the device C:.
- Commands that have optional switches use the forward slash (/) to deliminate between the command and each switch.
- 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 historical 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.

Even though the CLI has many commands and features, it cannot work together with the core of Windows or the GUI. 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.

To see more information about Windows PowerShell and get started using it, type **help** in PowerShell, as shown in the figure. You will be provided with much more information and resources to start using PowerShell.

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

---

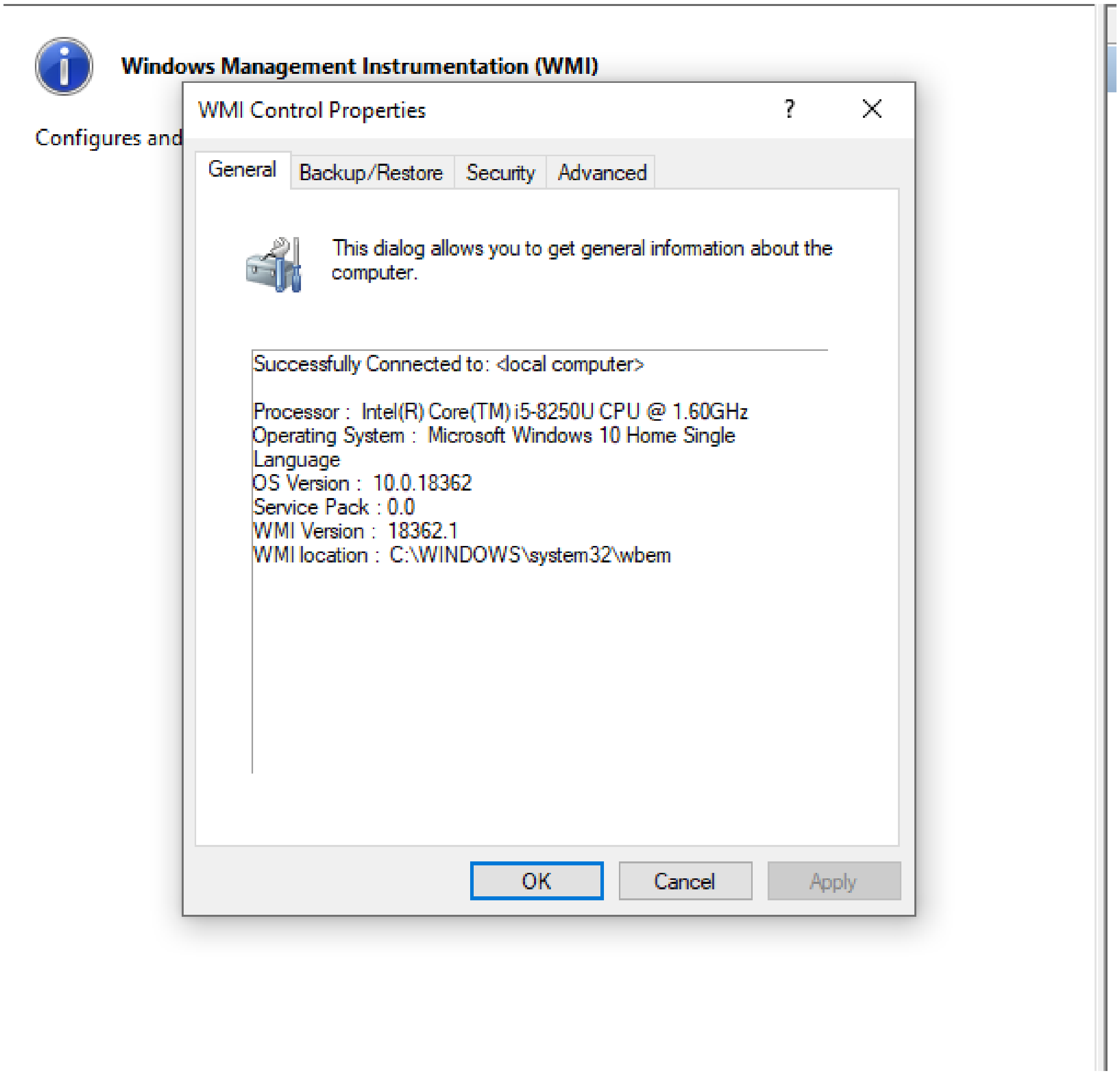
Windows Management Instrument

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. You can open WMI control by searching for computer management, and then right-click the **WMI Control** entry under **Services and Applications**, and choosing **Properties**. The WMI Control Properties window is shown in the figure.

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. Because of this, WMI access should be strictly limited.

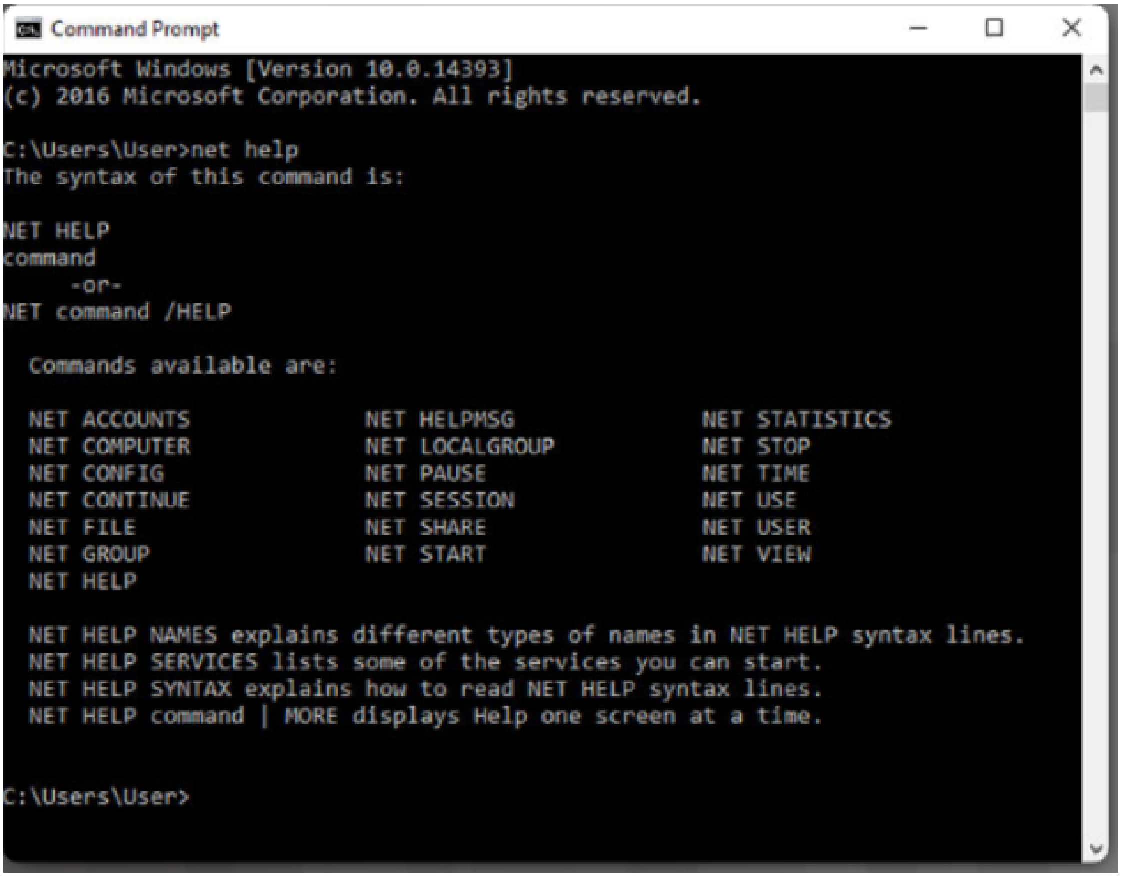


This dialog allows you to get general information about the computer.

```
Successfully Connected to: <local computer>

Processor :  Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz
Operating System :  Microsoft Windows 10 Home Single
Language
OS Version :  10.0.18362
Service Pack : 0.0
WMI Version :  18362.1
WMI location :  C:\WINDOWS\system32\wbem
```

Net command



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\User>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:\Users\User>
```

Windows has many commands that can be entered at the command line. One important command is the **net** command, used in the administration and maintenance of the OS. The **net** command supports many other commands 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 figure shows the commands that the **net** command can use. To see verbose help about any of the net commands, type **net help** *command*.

These are some common net commands:

- **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

Task manager and Resource Monitor

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. These tools also provide insight into the performance of the computer, such as CPU, memory, and network usage. These tools are especially useful when investigating a problem where malware is suspected. When a component is not performing the way that it should be, these tools can be used to determine what the problem might be.

Task Manager

The Task Manager, shown in Figure 1, provides a lot of information about what is running, and general performance of the computer. There are seven tabs in the Task Manager:

- **Processes** – All of the programs and processes that are currently running are shown here. The CPU, memory, disk, and network utilization of each process is displayed in columns. You can examine the properties of any of these processes, or end a process that 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 be. 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, shown in Figure 2. When searching for the reason a computer may be acting erratically, the Resource Monitor can help to find the source of the problem. The Resource Monitor has five tabs:

- **Overview** – General usage for each resource is shown in this tab. 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 in this tab. 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.

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, shown in Figure 1, is used. The easiest way to run this tool is to search for it and click it.

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.

To configure a network adapter, choose **Change adapter settings** to show all of the network connections that are available. Right-click the adapter you wish to configure and choose **Properties**, as shown in Figure 2. In the **This connection uses the following items:** box, highlight **Internet Protocol Version 4 (TCP/IPv4)** or **Internet Protocol Version 6 (TCP/IPv6)** depending on which version you wish to use (Figure 3). Click **Properties** to configure the adapter.

In the **Properties** dialogue box, shown in Figure 4, you can choose to **Obtain an address automatically** if there is a DHCP server available on the network. If you wish to configure addressing manually, you can fill in the address, subnet, default gateway, and DNS servers to configure the adapter. Click **OK** to accept the changes.

You can also use the **netsh.exe** tool to configure networking parameters from a command prompt. This program can display and modify the network configuration. Type **netsh /?** at the command prompt to see a list of all the switches that can be used with this command.

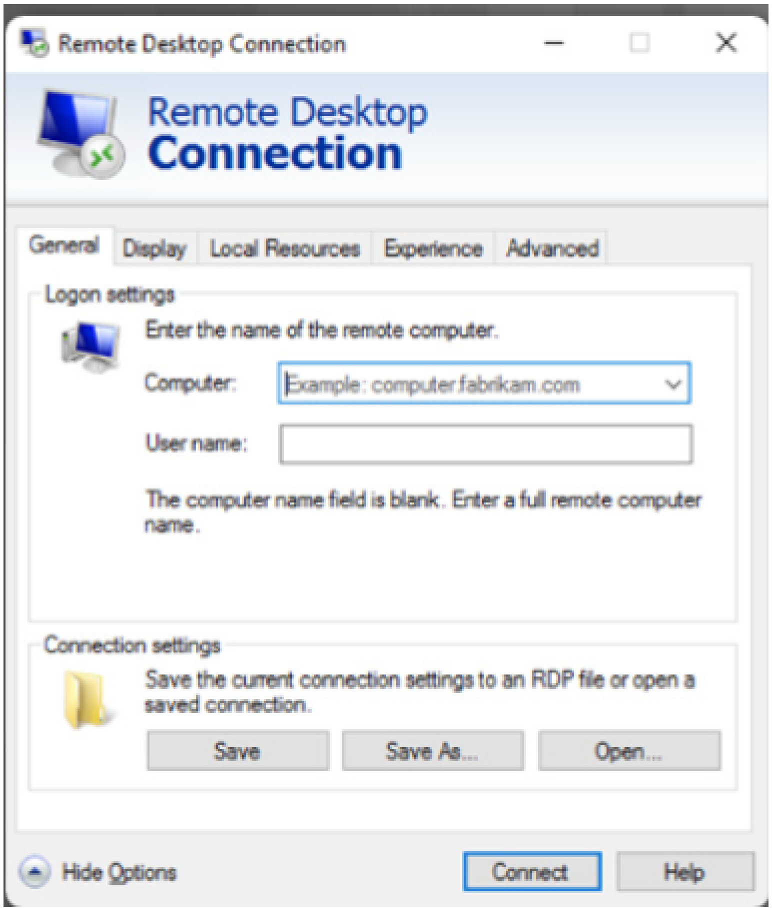
After the network configuration is complete, there are some basic commands that can be used to test connectivity to the local network, and the Internet. The most basic test is performed with the **ping** command. To test the adapter itself, type **ping 127.0.0.1** at the command prompt, as shown in Figure 5. This will make sure that the adapter is able to send and receive data. It also confirms that the TCP/IP protocol suite is properly installed in the computer. The 127.0.0.1 address is known as the loopback address.

Next, ping any host on the network. If you do not know any IP addresses of other hosts on the network, you can ping the default gateway. To find the address of the default gateway, type **ipconfig** at the command prompt, as shown in Figure 6. This command will return basic network information including the IP address of the host, the subnet mask, and the default gateway. You can also ping hosts on other connected networks to make sure that you have connectivity to those networks. The **ipconfig** command has many switches that are helpful when troubleshooting network issues. Type **ipconfig /?** to see a list of all the switches that can be used with this command.

When the ping command is issued, it will send four ICMP echo request messages to the indicated IP address. If there is no reply, there may be a problem with the network configuration. It is also possible that the intended host blocks ICMP echo requests. In this case, try to ping a different host on the network. Most often, there are four replies to the requests, showing the size of each request, the time it took to travel, and the time to live (TTL). TTL is the number of hops a packet takes along the path to its destination.

Domain Name System (DNS) should also be tested because it is used very often to find the address of hosts by translating it from a name. Use the nslookup command to test DNS. Type **nslookup cisco.com** at the command prompt to find the address of the Cisco 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, as shown in Figure 7. The **netstat** command will be examined further later in this chapter.

Accessing Network Resource



Logon settings

Enter the name of the remote computer.

Computer: Example: computer.fabrikam.com

User name:

The computer name field is blank. Enter a full remote computer name.

Connection settings

Save the current connection settings to an RDP file or open a saved connection.

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.

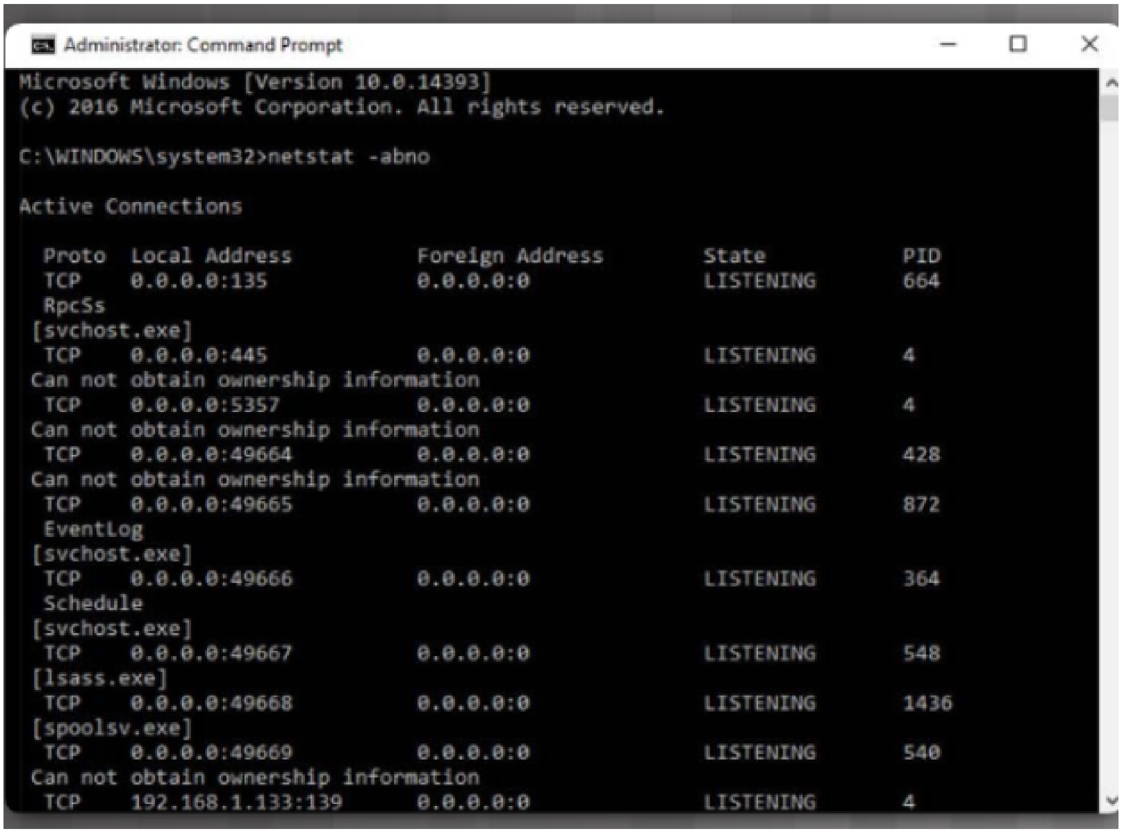
When sharing resources on the network, the area of the file system that will be shared will need to be identified. Access control can be applied to the folders and files to restrict users and groups to specific functions such as read, write, or deny. There are also special shares that are automatically created by Windows. These shares are called administrative shares. An administrative share is identified by the dollar sign ($) that comes after the share name. Each disk volume has an administrative share, represented by the volume letter and the $ such as C$, D$, or E$. The Windows installation folder is shared as admin$, the printers folder is shared as print$, and there are other administrative shares that can be connected. Only users with administrative privileges can access these shares.

The easiest way to connect to a share is to type the UNC of the share into the Windows File Explorer, in the box at the top of the screen which shows the breadcrumb listing of the current file system location. When Windows tries to connect to the share, you will be asked to provide credentials for accessing the resource. Remember that because the resource is on a remote computer, the credentials need to be for the remote computer, not the local computer.

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 with the computer. In Windows, this function is known as the Remote Desktop Protocol (RDP). When investigating security incidents, a security analyst uses RDP often to access remote computers. 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.

2.2.2 Windows Security

Netstat command



```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>netstat -abno

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       664
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING       4
 Can not obtain ownership information
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       428
 Can not obtain ownership information
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       872
  EventLog
 [svchost.exe]
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       364
  Schedule
 [svchost.exe]
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       548
 [lsass.exe]
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       1436
 [spoolsv.exe]
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       540
 Can not obtain ownership information
  TCP    192.168.1.133:139      0.0.0.0:0              LISTENING       4
```

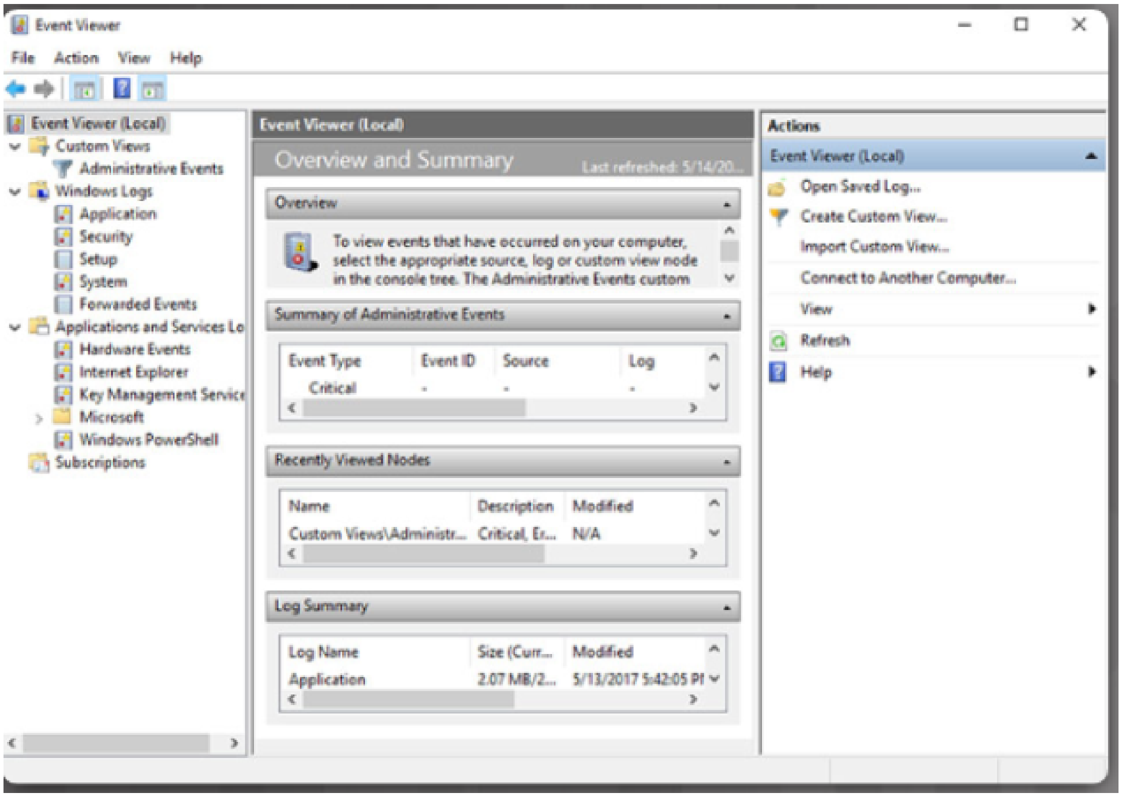
When malware is present in a computer, it will often open communication ports on the host to send and receive data. The **netstat** command can be used to look for inbound or outbound connections that are not authorized. When used on its own, the **netstat** command will display all of the active TCP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

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 the 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 in the Task Manager. To do this, open a command prompt with administrative privileges and use the command **netstat -abno**, as shown in the figure.

By examining the active TCP connections, an analyst should be able to determine if there are any suspicious programs that are listening for incoming connections on the host. You can also trace that process to the Windows Task Manager and cancel the process. There may be more than one process listed with the same name. If this is the case, use the PID to find the correct process. Each process running on the computer has a unique PID. 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



Overview

To view events that have occurred on your computer, select the appropriate source, log or custom view node in the console tree. The Administrative Events custom

Summary of Administrative Events

Event Type	Event ID	Source	Log
Critical	-	-	-

Recently Viewed Nodes

Name	Description	Modified
Custom Views\Administr...	Critical, Er...	N/A

Log Summary

Log Name	Size (Curr...	Modified
Application	2.07 MB/2...	5/13/2017 5:42:05 PI

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.

It is also possible to create a custom view. This is useful when looking for certain types of events, finding events that happened during a certain time period, displaying events of a certain level, and many other criteria. 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.

Windows Update

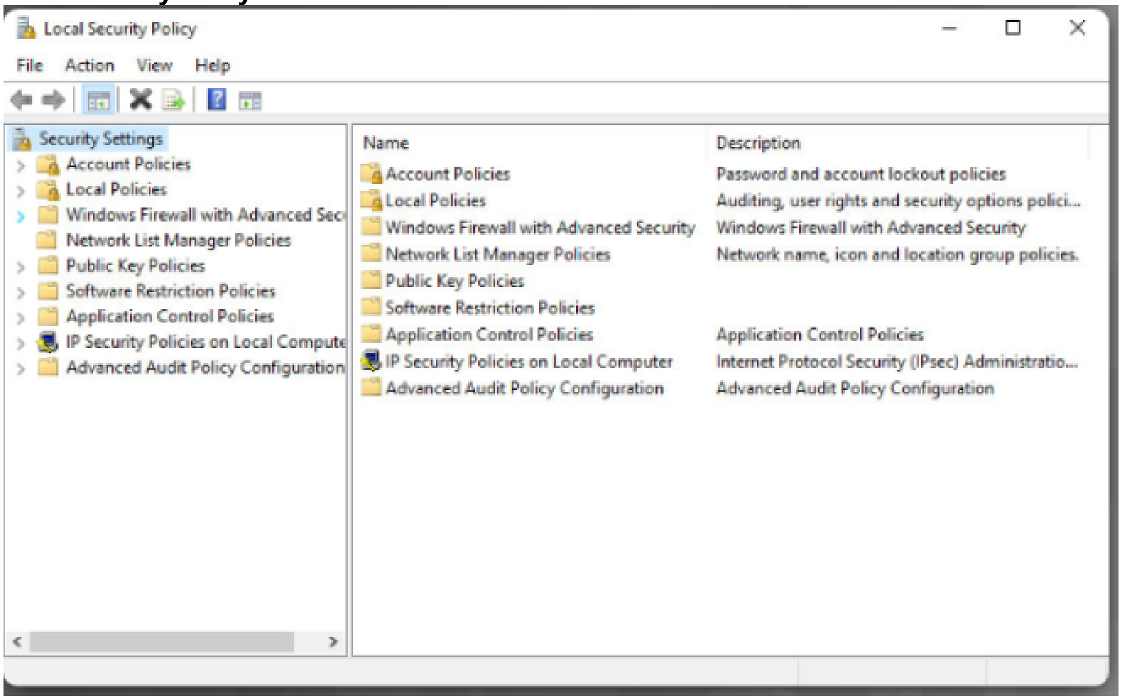
No software is perfect, and the Windows operating system is no exception. Attackers are constantly coming up with new ways to compromise computers and exploit bad code. Some of these attacks come so quickly that there is no defense against them. These are called zero-day exploits. Microsoft and security 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. From time to time, manufacturers combine patches and upgrades into a comprehensive update application called a service pack. Many devastating virus attacks could have been much less severe if more users had downloaded and installed the latest service pack.

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. Depending on the setting you choose, Windows automatically downloads and installs any high-priority updates that your computer needs or notifies you as these updates become available. To configure the settings for Windows update, search for Windows Update and click the application.

The Update status, shown in the figure, allows you to check for updates manually and see the update history of the computer. There are also settings for the hours where the computer will not automatically restart, for example during regular business hours. You can also choose when to restart the computer after an update, if necessary, with the Restart options. Advanced options are also available to choose how updates are installed and get updates for other Microsoft products.

Local Security Policy


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Windows Firewall with Advanced Sec
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options polici...
Windows Firewall with Advanced Security	Windows Firewall with Advanced Security
Network List Manager Policies	Network name, icon and location group policies.
Public Key Policies	
Software Restriction Policies	
Application Control Policies	Application Control Policies
IP Security Policies on Local Computer	Internet Protocol Security (IPsec) Administratio...
Advanced Audit Policy Configuration	Advanced Audit Policy Configuration

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**. To open the Local Security Policy applet, search for Local Security Policy and click the program.

Password guidelines are an important component of a security policy. Any user that must log on to a computer or connect to a network resource should be required to have a password. Passwords help prevent theft of data and malicious acts. Passwords also help to confirm that the logging of events is valid by ensuring that the user is the person they say that they are. Password

Policy is found under Account Policies, and defines the criteria for the passwords for all of the users on the local computer.

Use the **Account Lockout Policy i**n Account Policies to **prevent brute-force login attempts.** You can set the policy to allow the user to enter a wrong username and/or password five times. After five attempts, the account is locked out for 30 minutes. After 30 minutes, the number of attempts is reset to zero and the user can attempt to login again.

It is important to make sure that computers are secure when users are away. A security policy should contain a rule about requiring a computer to lock when the screensaver starts. This will ensure that after a short time away from the computer, the screen saver will start and then the computer cannot be used until the user logs in.

If the Local Security Policy on every stand-alone computer is the same, then use the Export Policy feature. Save the policy with a name, such as workstation.inf. Copy the policy file to an external media or network drive to use on other stand-alone computers. This is particularly helpful if the administrator needs to configure extensive local policies for user rights and security options.

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 Server

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:

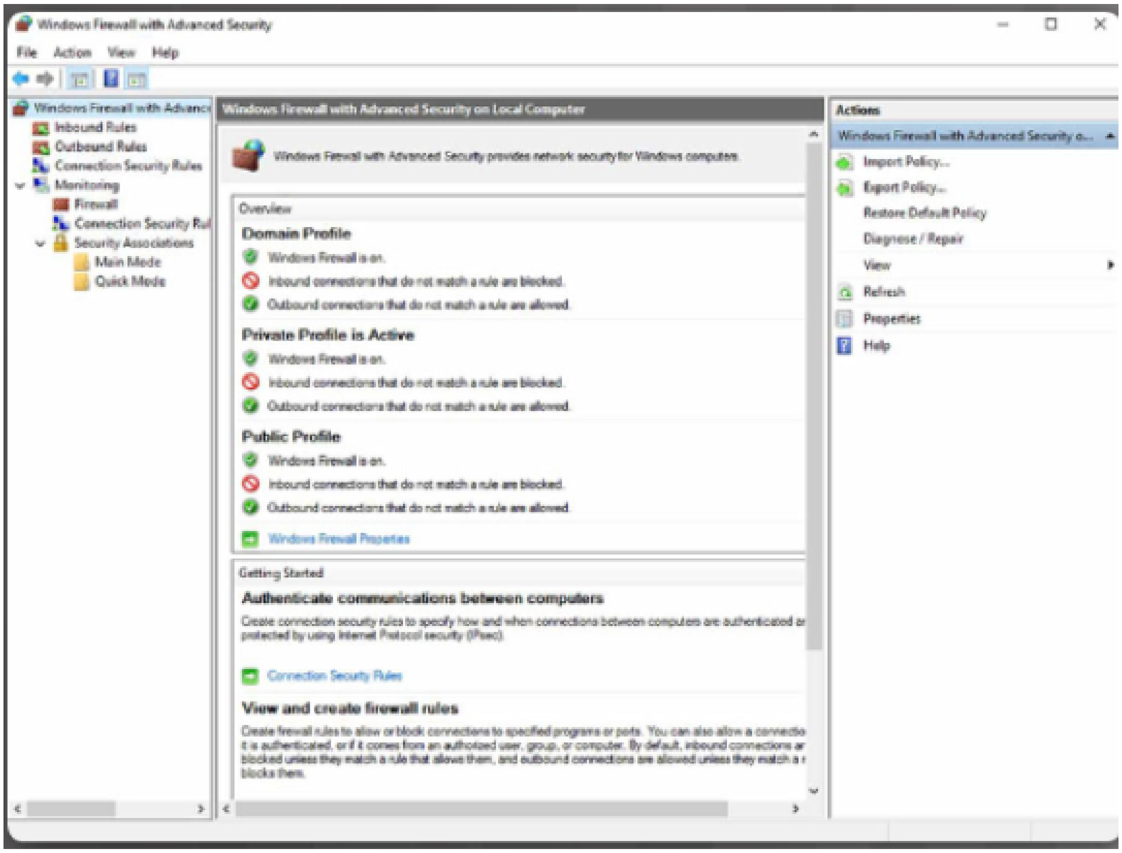
- **Antivirus protection** – This program continuously monitors for viruses. When a virus is detected, the user is warned, and the program attempts to quarantine or delete the virus.
- **Adware protection** – This program continuously looks for programs that display advertising on your computer.
- **Phishing 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.

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

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, shown in the figure. Windows Defender is turned on by default providing real-time protection against infection.

To open Windows Defender, search for it and click the program. Although Windows Defender works in the background, you can perform manual scans of the computer and storage devices. You can also manually update the virus and spyware definitions in the **Update** tab. Also, to see all of the items that were found during previous scans, click the **History** tab.

FIrewall



Windows Firewall with Advanced Security on Local Computer

Windows Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

✓ Windows Firewall is on.

🚫 Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

Private Profile is Active

✓ Windows Firewall is on.

🚫 Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

Public Profile

✓ Windows Firewall is on.

🚫 Inbound connections that do not match a rule are blocked.

✓ Outbound connections that do not match a rule are allowed.

Windows Firewall Properties

Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authenticated ar protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

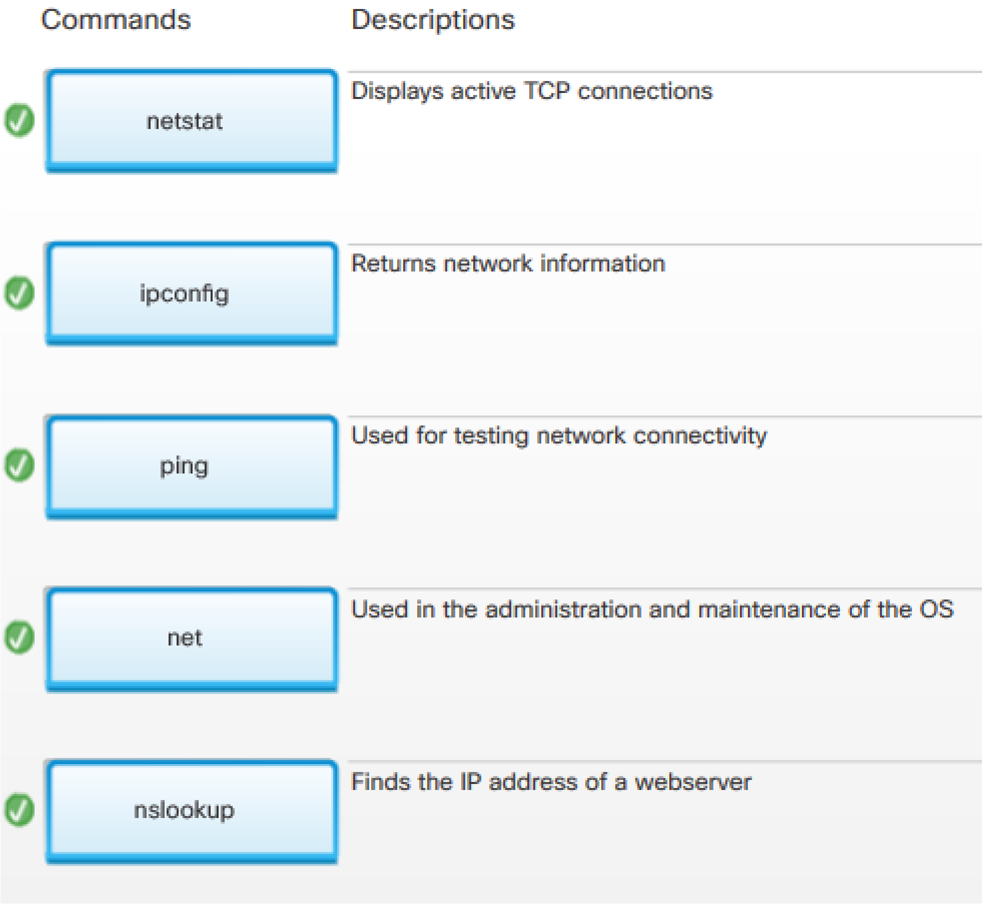
Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connectio it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections ar blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a r blocks them.

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. In the past, software and hardware were shipped with permissive settings. As users neglected to configure their equipment, the default permissive settings left many devices exposed to attackers. Most devices now ship with settings as restrictive as possible, while still allowing easy setup.

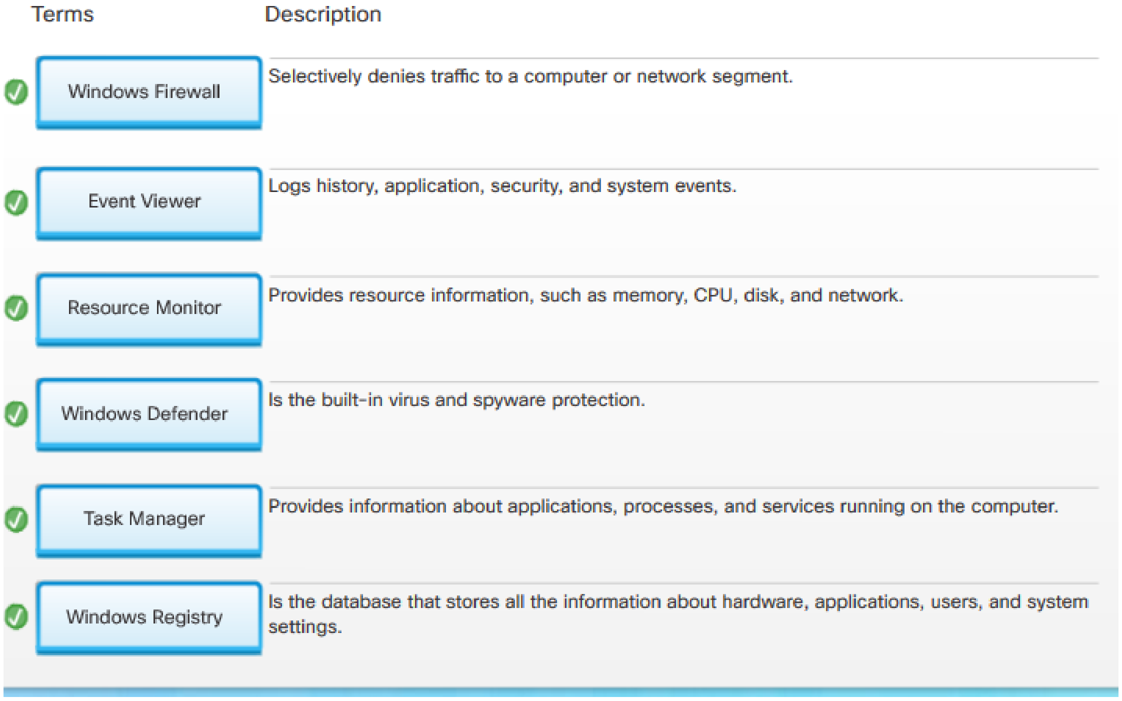
To allow program access through the Windows Firewall, search for Windows Firewall, click its name to run it, and click **Allow an app or feature through Windows Firewall**, as shown in Figure 1.

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**.

Many additional settings can be found under **Advanced settings**, as shown in Figure 2. Here you can create inbound or outbound traffic rules based on different criteria. You can also import and export policies or monitor different aspects of the firewall.



	Commands	Descriptions
✓	netstat	Displays active TCP connections
✓	ipconfig	Returns network information
✓	ping	Used for testing network connectivity
✓	net	Used in the administration and maintenance of the OS
✓	nslookup	Finds the IP address of a webserver



	Terms	Description
✓	Windows Firewall	Selectively denies traffic to a computer or network segment.
✓	Event Viewer	Logs history, application, security, and system events.
✓	Resource Monitor	Provides resource information, such as memory, CPU, disk, and network.
✓	Windows Defender	Is the built-in virus and spyware protection.
✓	Task Manager	Provides information about applications, processes, and services running on the computer.
✓	Windows Registry	Is the database that stores all the information about hardware, applications, users, and system settings.

Conclusion

In this chapter, you learned about the history and architecture of the Windows operating system. There have been over 40 versions of Windows desktop, Windows server, and Windows mobile operating systems.

HAL handles all the communication between the hardware and the kernel. The CPU can operate in two separate modes: kernel mode and user mode. Applications that are installed are run in user mode, and operating system code runs in kernel mode.

NTFS formats the disk into four important data structures:

- Partition Boot Sector
- Master File Table (MFT)
- System Files
- File Area

Applications are generally made up of many processes. A process is any program that is currently executing. Each running process is made up of at least one thread. A thread is a part of the process that can be executed. Some of the processes that Windows runs are services. These are programs that run in the background to support the operating system and applications.

Each process in a 32-bit Windows computer supports a virtual address space that enables addressing up to four gigabytes. Each process in a 64-bit Windows computer supports a virtual address space of up to eight terabytes.

Windows stores all of the information about hardware, applications, users, and system settings in a large database known as the registry. The registry is a hierarchical database where the highest level is known as a hive. These are the five hives of the Windows registry:

- HKEY_CURRENT_USER (HKCU)
- HKEY_USERS (HKU)
- HKEY_CLASSES_ROOT (HKCR)
- HKEY_LOCAL_MACHINE (HKLM)
- HKEY_CURRENT_CONFIG (HKCC)

In this chapter, you also learned how to configure, monitor, and keep Windows secure. To do this normally requires that you run programs as Administrator. As administrator, you can create users and groups, disable access to the administrator and guest accounts, and use a variety of administrator tools including:

- All commands available to CLI and PowerShell
- Remote computer management using WMI and Remote Desktop
- Task Manager and Resource Monitor
- Networking configuration

As administrator, you will also have the ability to use all the Windows security tools including:

- The **netstat** command to look for inbound and outbound connections that are not authorized
- Event Viewer for access to logs that document the history of application, security, and system events
- Windows Update configuration and scheduling
- Windows Local Security Policy to secure stand-alone computers that are not part of an Active Directory domain
- Windows Defender configuration for built-in virus and spyware protection
- Windows Firewall configuration to fine-tune the default settings

As a cybersecurity analyst, you need a basic understanding of how Windows operates and what tools are available to help keep Windows endpoints secure.