

Chapter 2: Windows Operating System

Cybersecurity Operations v1.1



Chapter 2 - Sections & Objectives

- 2.1 Windows Overview
 - Explain the operation of the Windows Operating System.
 - Describe the history of the Windows Operating System.
 - Explain the architecture of Windows and its operation.
- 2.2 Windows Administration
 - Explain how to secure Windows endpoints.
 - Explain how to configure and monitor Windows.
 - Explain how Windows can be kept secure.

2.1 Windows Overview

Disk Operating System

- Disk Operating System (DOS) - operating system that the computer uses to enable data storage devices to read and write files.
- MS-DOS, created by Microsoft, used a command line as the interface for people to create programs and manipulate data files.
- Early versions of Windows consisted of a Graphical User Interface (GUI) that ran over MS-DOS
- In newer versions of Windows, built on NT, the operating system itself is in direct control of the computer and its hardware.

```
Starting MS-DOS...

HIMEM is testing extended memory...done.

C:\>C:\DOS\SMARTDRV.EXE /X
C:\>dir

Volume in drive C is MS-DOS_6
Volume Serial Number is 4AA6-6939
Directory of C:\

DOS             <DIR>              05-06-17   1:09p
COMMAND.COM     54,645 05-31-94   6:22a
WINA20          386      9,349 05-31-94   6:22a
CONFIG.SYS      71      05-06-17   1:10p
AUTOEXEC.BAT    78      05-06-17   1:10p
                5 file(s)          64,143 bytes
                517,021,696 bytes free

C:\>_
```

Windows Versions

- Since 1993, there have been more than 20 releases of Windows that are based on the NT operating system.
- Beginning with Windows XP, a 64-bit edition was available.
- 64-bit Windows can theoretically address 16.8 million terabytes of RAM
- With each subsequent release of Windows, the operating system has become more refined by incorporating more features.

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

Windows History

Windows GUI



- Windows has a graphical user interface (GUI) for users to work with data files and software.
- Main section of the GUI is the desktop, which contains the Task Bar
- Task Bar includes the Start Menu and Search, Quick Launch items and Notifications Area.
- Right-clicking an icon will bring up additional list of functions, known as a Context Menu.
- Windows File Explorer, is a tool used to navigate the entire file system of a computer.

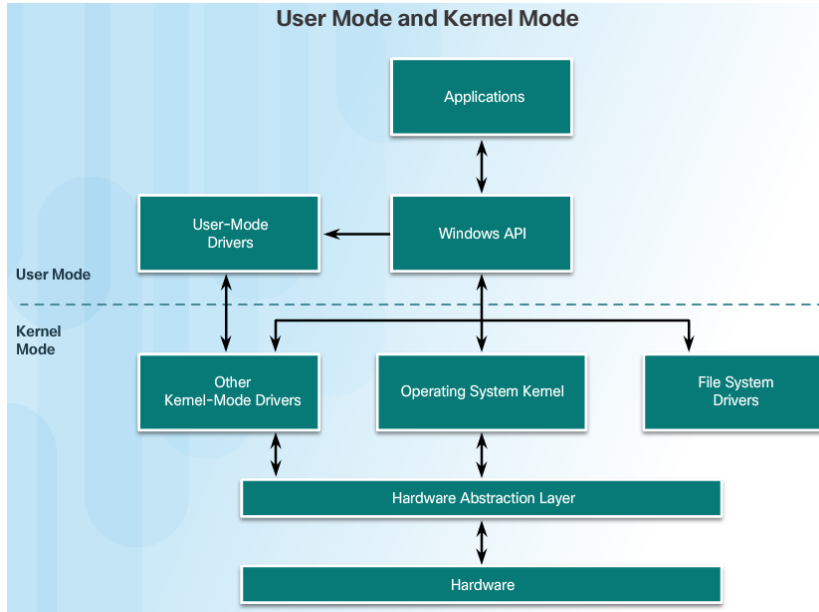
Operating System Vulnerabilities

- To take advantage of an operating system vulnerability, the attacker must use a technique or a tool to exploit the vulnerability.
- Common Windows OS Security Recommendations:
 - Implement virus or malware protection.
 - Do not allow unknown or unmanaged services.
 - Use encryption.
 - Implement a strong security policy.
 - Review firewall settings periodically.
 - Set File and Share permissions correctly.
 - Use strong passwords.
 - Login as Administrator only when necessary.



Windows Architecture and Operations

Hardware Abstraction Layer

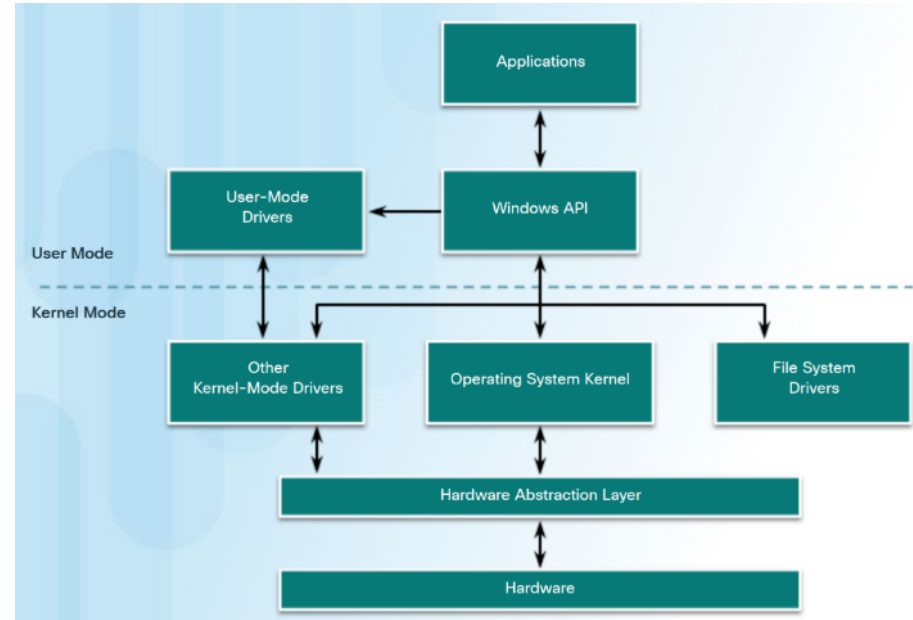


- A hardware abstraction layer (HAL) is code that handles all of the communication between the hardware and the kernel.
- The kernel is the core of the operating system and has control over the entire computer.
- The kernel handles all of the input and output requests, memory, and all of the peripherals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

Windows Architecture and Operations

User Mode and Kernel Mode

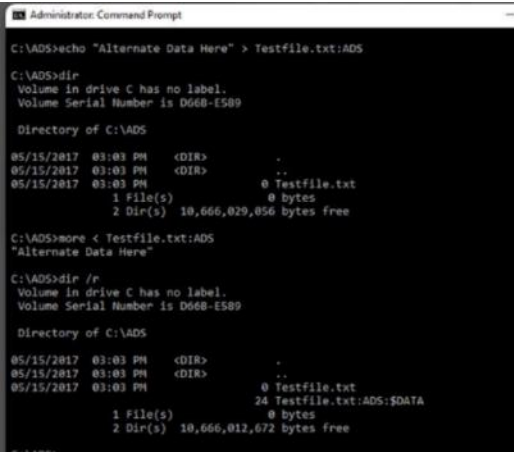
- There are two different modes in which a CPU operates when the computer has Windows installed: the user mode and the kernel mode.
- Installed applications run in user mode, and operating system code runs in kernel mode.



Windows Architecture and Operations

Windows File Systems

- A file system is how information is organized on storage media.
 - Windows supports the following file systems:
 - File Allocation Table (FAT)
 - exFAT
 - Hierarchical File System Plus (HFS+)
 - Extended File System (EXT)
 - New Technology File System (NTFS)
- 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.
- 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.



```
Administrator: Command Prompt

C:\>echo "Alternate Data Here" > Testfile.txt:ADS

C:\>dir
Volume in drive C has no label.
Volume Serial Number is D668-1589

Directory of C:\>

05/15/2017  03:03 PM    <DIR>          .
05/15/2017  03:03 PM    <DIR>          ..
05/15/2017  03:03 PM                0 Testfile.txt
                   1 File(s)                0 bytes
                   2 Dir(s)  10,666,029,856 bytes free

C:\>more < Testfile.txt:ADS
"Alternate Data Here"

C:\>dir /p
Volume in drive C has no label.
Volume Serial Number is D668-1589

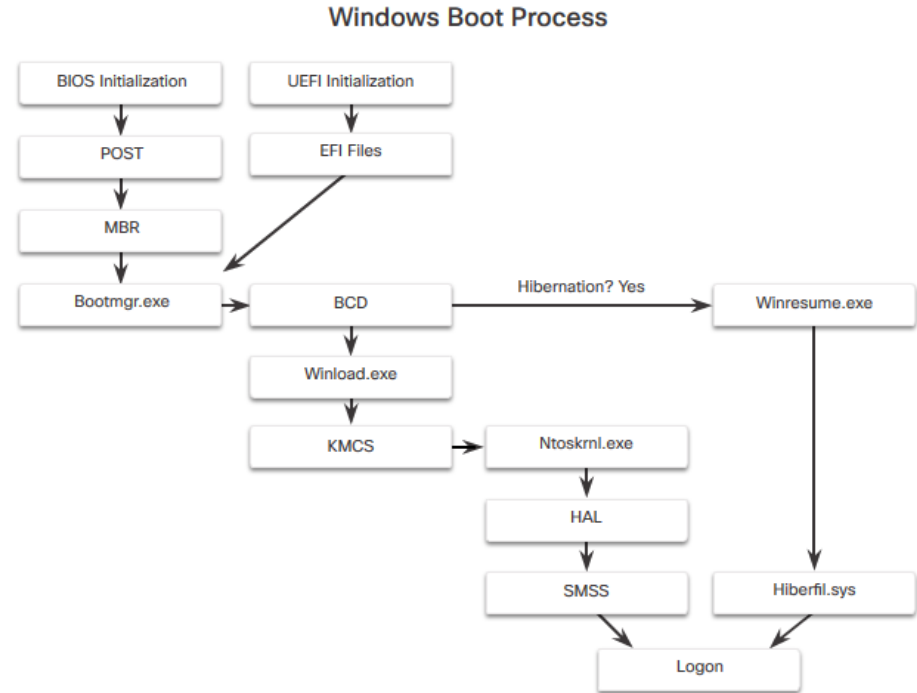
Directory of C:\>

05/15/2017  03:03 PM    <DIR>          .
05/15/2017  03:03 PM    <DIR>          ..
05/15/2017  03:03 PM                0 Testfile.txt
                   1 File(s)                0 bytes
                   2 Dir(s)  10,666,012,672 bytes free
```

Windows Architecture and Operations

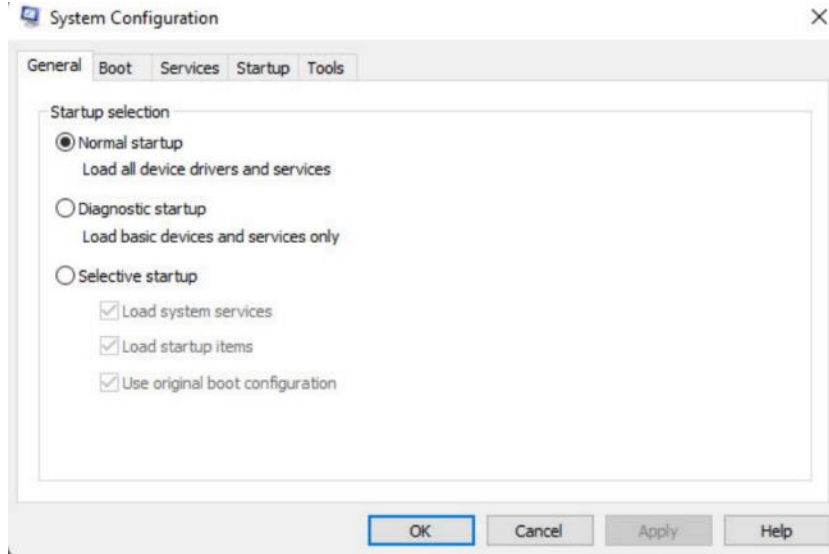
Windows Boot Process

- Two types of computer firmware exist: Basic Input-Output System (BIOS) and Unified Extended Firmware Interface (UEFI)
- UEFI was designed to replace BIOS and support the new features.
- Whether BIOS or UEFI, after a valid Windows installation is located, the Bootmgr.exe file is run.



Windows Architecture and Operations

Windows Startup and Shutdown

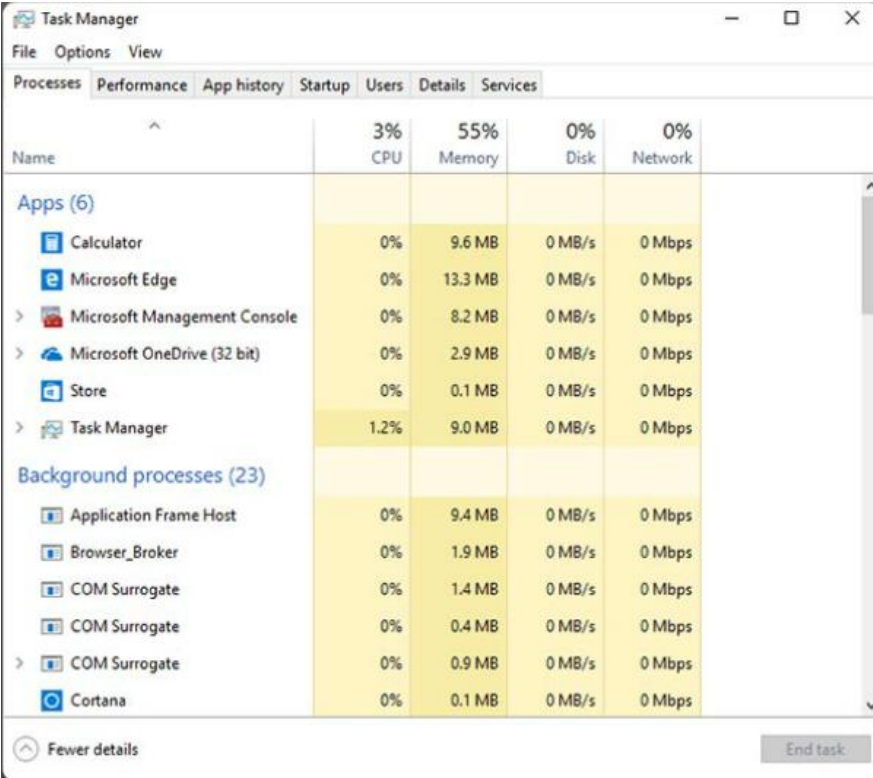


- Different entries in these registry locations define which services and applications will start, as indicated by their entry type.
 - HKEY_LOCAL_MACHINE
 - HKEY_CURRENT_USER
- These types include Run, RunOnce, RunServices, RunServicesOnce, and Userinit.
- There are five tabs which contain the configuration options:
 - General
 - Boot
 - Services
 - Startup
 - Tools
- It is always best to perform a proper shutdown to turn off the computer.

Windows Architecture and Operations

Processes, Threads, and Services

- A process is any program that is currently executing.
- A thread is a part of the process that can be executed.
- In Windows multiple threads can be executed at the same time.
- Some of the processes that Windows runs are services - programs that run in the background to support the operating system and applications.

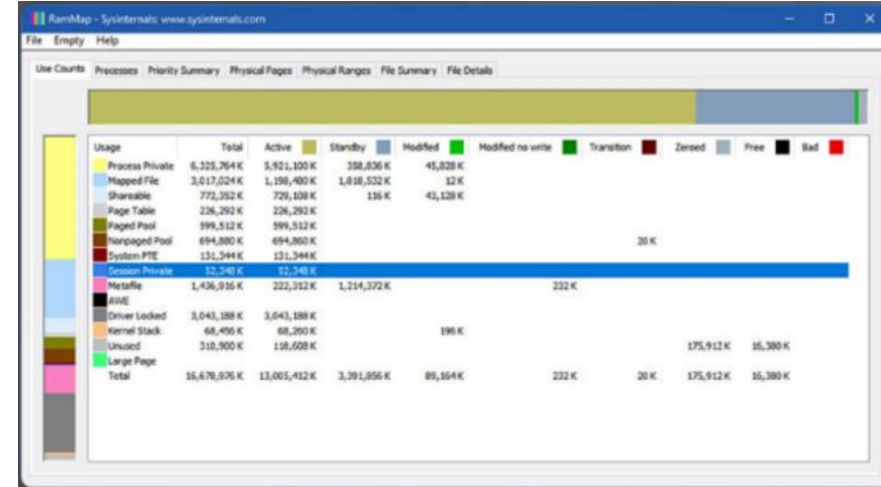


Name	3% CPU	55% Memory	0% Disk	0% Network
Apps (6)				
Calculator	0%	9.6 MB	0 MB/s	0 Mbps
Microsoft Edge	0%	13.3 MB	0 MB/s	0 Mbps
Microsoft Management Console	0%	8.2 MB	0 MB/s	0 Mbps
Microsoft OneDrive (32 bit)	0%	2.9 MB	0 MB/s	0 Mbps
Store	0%	0.1 MB	0 MB/s	0 Mbps
Task Manager	1.2%	9.0 MB	0 MB/s	0 Mbps
Background processes (23)				
Application Frame Host	0%	9.4 MB	0 MB/s	0 Mbps
Browser_Broker	0%	1.9 MB	0 MB/s	0 Mbps
COM Surrogate	0%	1.4 MB	0 MB/s	0 Mbps
COM Surrogate	0%	0.4 MB	0 MB/s	0 Mbps
COM Surrogate	0%	0.9 MB	0 MB/s	0 Mbps
Cortana	0%	0.1 MB	0 MB/s	0 Mbps

Windows Architecture and Operations

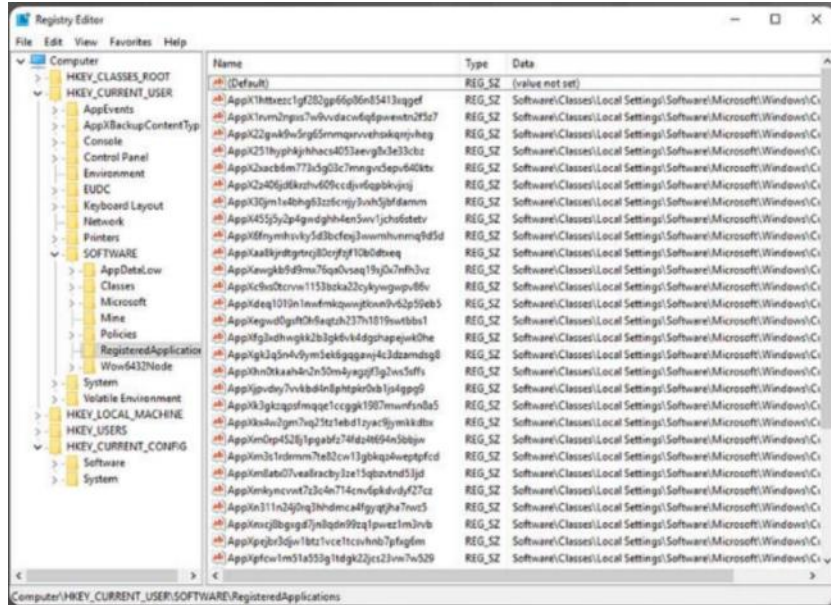
Memory Allocation and Handles

- The virtual address space for a process is the set of virtual addresses that the process can use.
- Each process in a 32-bit Windows computer supports a virtual address space that enables addressing up to 4 gigabytes.
- Each process in a 64-bit Windows computer supports a virtual address space of 8 terabytes.
- Each user space process runs in a private address space, separate from other user space processes.
- Sysinternals's RamMap – Used to view memory allocation.



Windows Architecture and Operations

The Windows Registry



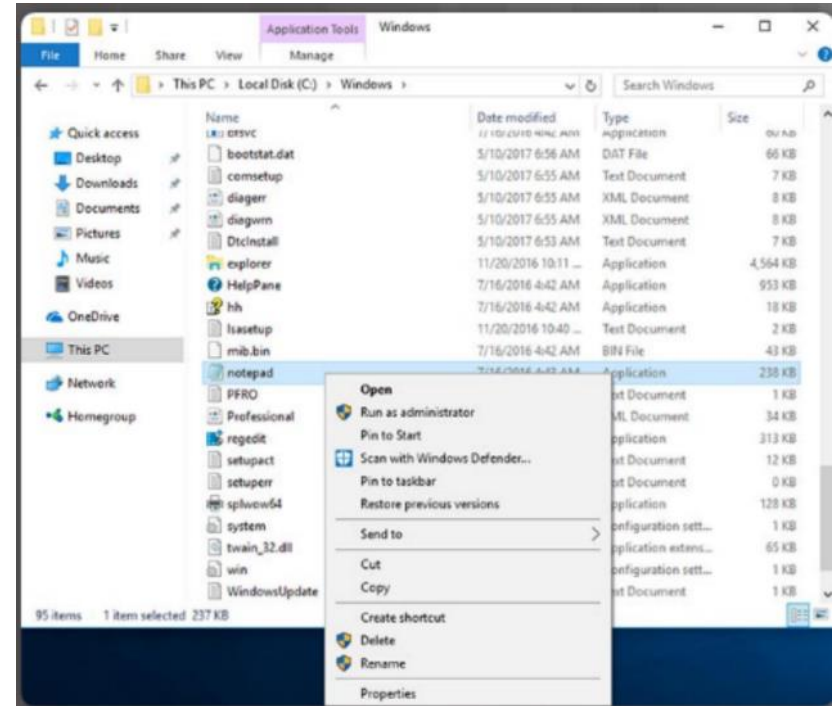
- Information about hardware, applications, users, and system settings is stored in the Windows registry.
- The registry is a hierarchical database where the highest level is known as a hive, below that there are keys, followed by subkeys.
- The five hives of the Windows registry:
 - HKEY_CURRENT_USER (HKCU)** - Holds data concerning the currently logged in user.
 - HKEY_USERS (HKU)** - Holds data concerning all the user accounts.
 - 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.
- Navigation is very similar to Windows file explorer.

2.2 Windows Administration

Windows Configuration and Monitoring

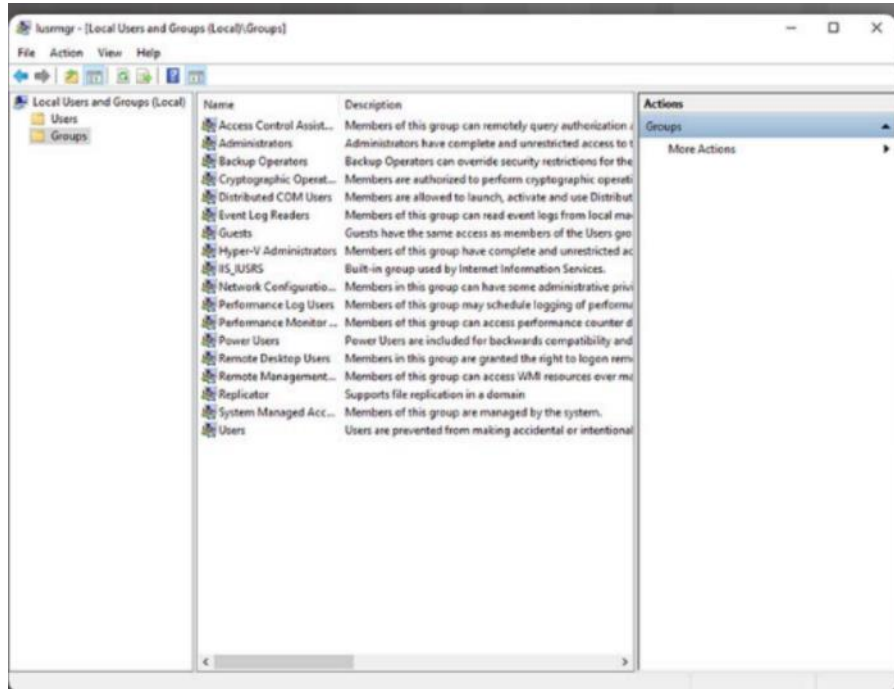
Run as Administrator

- Sometimes, it is necessary to run or install software that requires the privileges of the Administrator.
- Use “Run as administrator” or open an Administrator Command Prompt.



Windows Configuration and Monitoring

Local Users and Domains

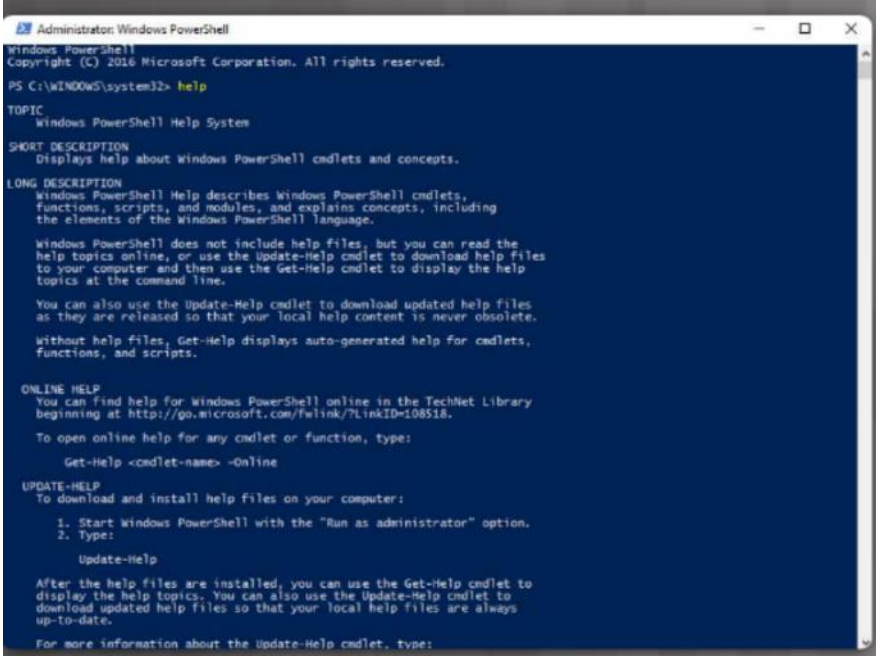


- Local users and groups are managed with the lusrmgr.msc control panel applet.
- A group is named and has a specific set of permissions associated with it. A user placed into a group will have the permissions of that group assigned to them.
- A domain - type of network service where all of the users, groups, computers, peripherals, and security settings are stored on and controlled by a database.
 - This database is stored on computers or groups of computers called domain controllers (DCs).

Windows Configuration and Monitoring

CLI and PowerShell

- The Windows command line interface (CLI) can be used to run programs, navigate the file system, and manage files and folders.
- Another environment, called the Windows PowerShell, can be used to create scripts to automate tasks that the regular CLI is unable to create.

A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The window has a blue background and white text. It shows the output of the 'help' command, displaying information about the Windows PowerShell Help System, including a short description, long description, online help resources, and update instructions.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> help

TOPIC
    Windows PowerShell Help System

SHORT DESCRIPTION
    Displays help about Windows PowerShell cmdlets and concepts.

LONG DESCRIPTION
    Windows PowerShell Help describes Windows PowerShell cmdlets,
    functions, scripts, and modules, and explains concepts, including
    the elements of the Windows PowerShell language.

    Windows PowerShell does not include help files, but you can read the
    help topics online, or use the Update-Help cmdlet to download help files
    to your computer and then use the Get-Help cmdlet to display the help
    topics at the command line.

    You can also use the Update-Help cmdlet to download updated help files
    as they are released so that your local help content is never obsolete.

    Without help files, Get-Help displays auto-generated help for cmdlets,
    functions, and scripts.

ONLINE HELP
    You can find help for Windows PowerShell online in the TechNet Library
    beginning at http://go.microsoft.com/fwlink/?LinkID=108518.

    To open online help for any cmdlet or function, type:

        Get-Help <cmdlet-name> -Online

UPDATE-HELP
    To download and install help files on your computer:

        1. Start Windows PowerShell with the "Run as administrator" option.
        2. Type:

            Update-Help

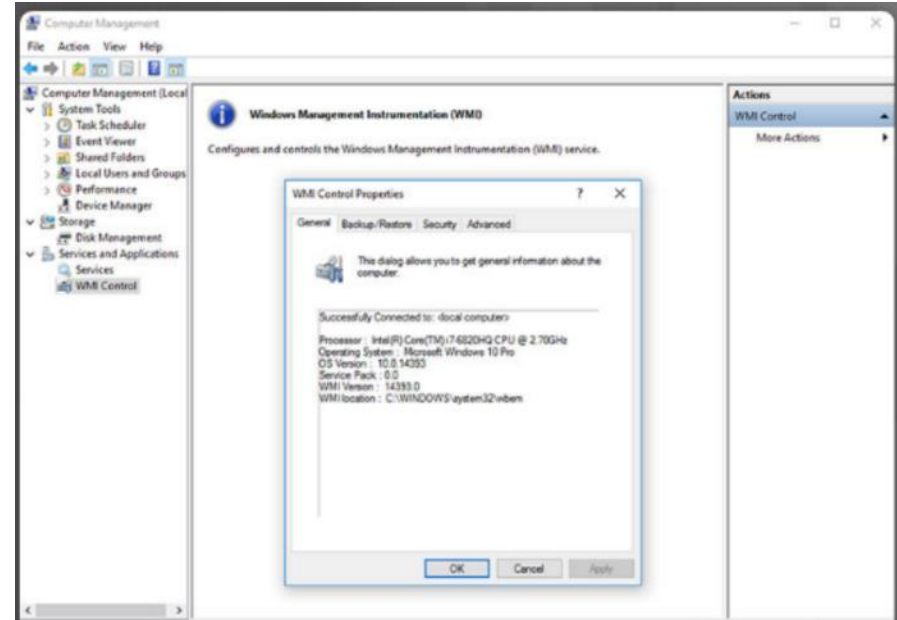
    After the help files are installed, you can use the Get-Help cmdlet to
    display the help topics. You can also use the Update-Help cmdlet to
    download updated help files so that your local help files are always
    up-to-date.

    For more information about the Update-Help cmdlet, type:
```

Windows Configuration and Monitoring

Windows Management Instrumentation

- Windows Management Instrumentation (WMI) is used to manage remote computers.
- Some attacks today use WMI to connect to remote systems, modify the registry, and run commands, therefore access should be strictly limited.



The net Command

- The **net** command supports many other commands that follow the **net** command and can be combined with switches to focus on specific output.

```
Commands available are:

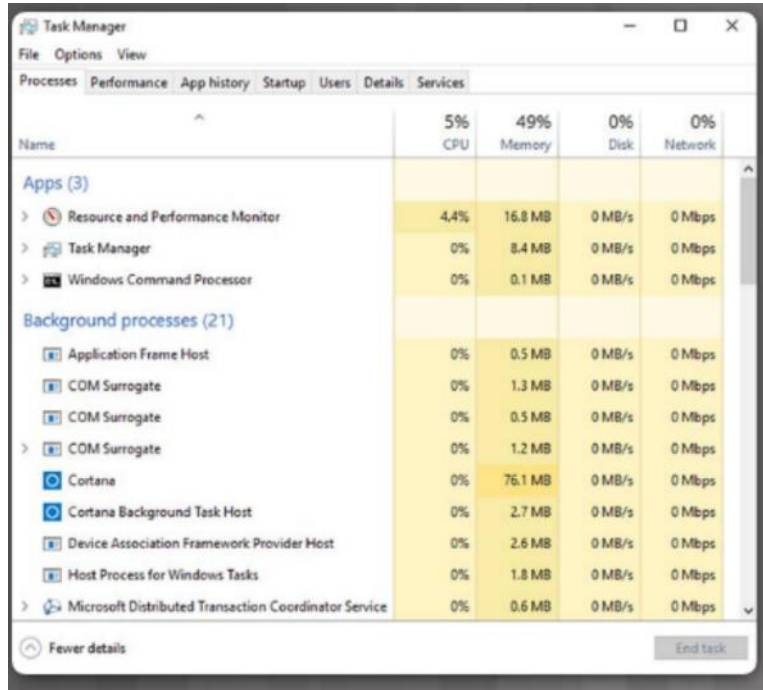
NET ACCOUNTS          NET HELPMSG          NET STATISTICS
NET COMPUTER          NET LOCALGROUP      NET STOP
NET CONFIG            NET PAUSE           NET TIME
NET CONTINUE          NET SESSION         NET USE
NET FILE              NET SHARE           NET USER
NET GROUP             NET START           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.
```

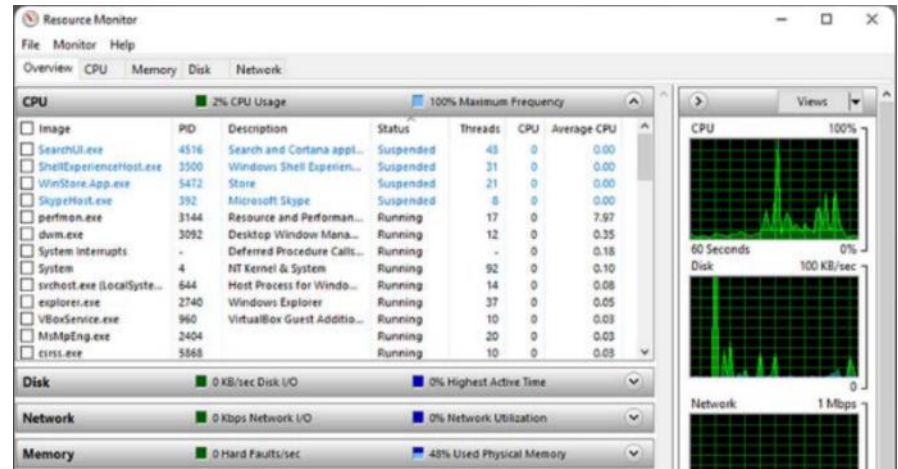
- To see a list of the **net** commands, type **net help** at the command prompt.

Windows Configuration and Monitoring

Task Manager and Resource Monitor



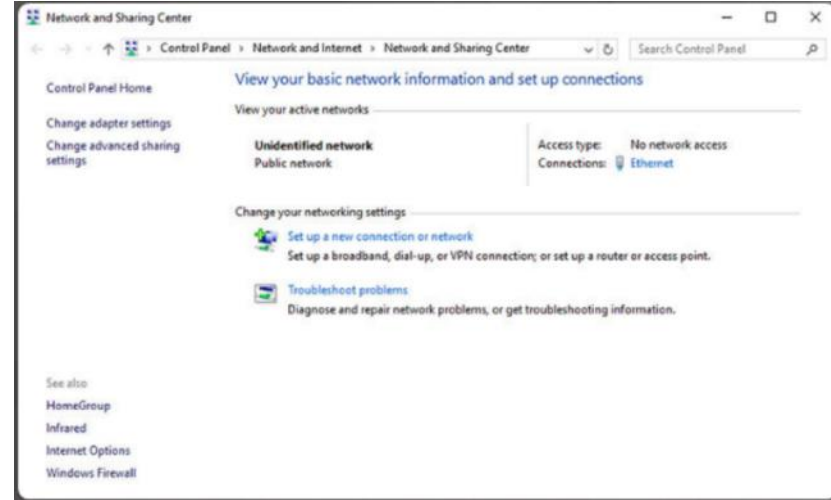
- Task Manager provides a lot of information about what is running, and general performance of the computer.
- Resource Monitor is used when more detailed information about resource usage is needed.



Windows Configuration and Monitoring

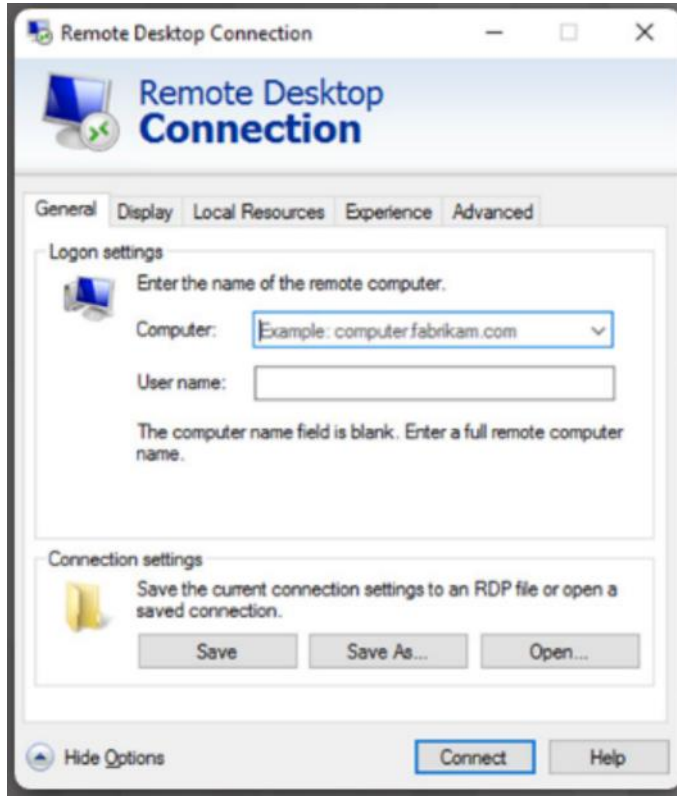
Networking

- To configure Windows networking properties and test networking settings, the Network and Sharing Center is used.
- Use the **netsh.exe** tool to configure networking parameters from a command prompt.
- To test the network adapter, type **ping 127.0.0.1** at the command prompt.
- Domain Name System (DNS) should also be tested using **nslookup** command.
- Use **netstat** at the command line to see details of active network connections.



Windows Configuration and Monitoring

Accessing Network Resources



- Server Message Block (SMB) protocol is used to share network resources.
- Universal Naming Convention (UNC) format is used to connect to resources.
- An administrative share is identified by the dollar sign (\$) that comes after the share name.
- Remote Desktop Protocol (RDP) can be used to log onto a remote host and make configuration changes, install software, or troubleshoot.

Windows Configuration and Monitoring

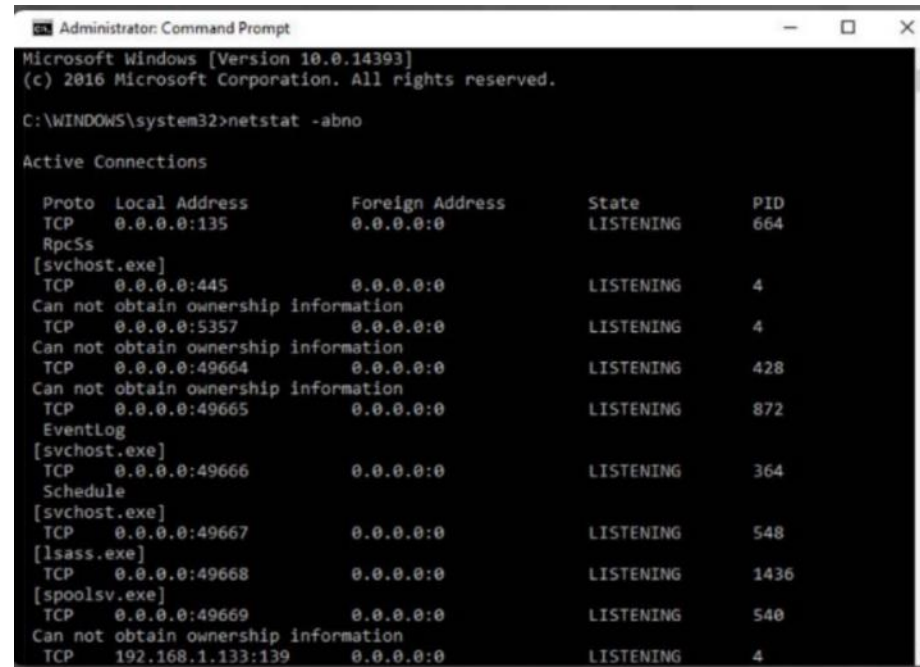
Windows Server

- There is another edition of Windows that is mainly used in data centers called Windows Server.
- Services that Windows Server hosts include:
 - Network Services
 - File Services
 - Web Services
 - Management



The netstat Command

- The **netstat** command can be used to look for inbound or outbound connections that are not authorized.
- Link the connections to the running processes in the Task Manager by using **netstat -abno**
- To display the Process IDs for the processes in the Task Manager, open the Task Manager, right-click the table heading and select PID.



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

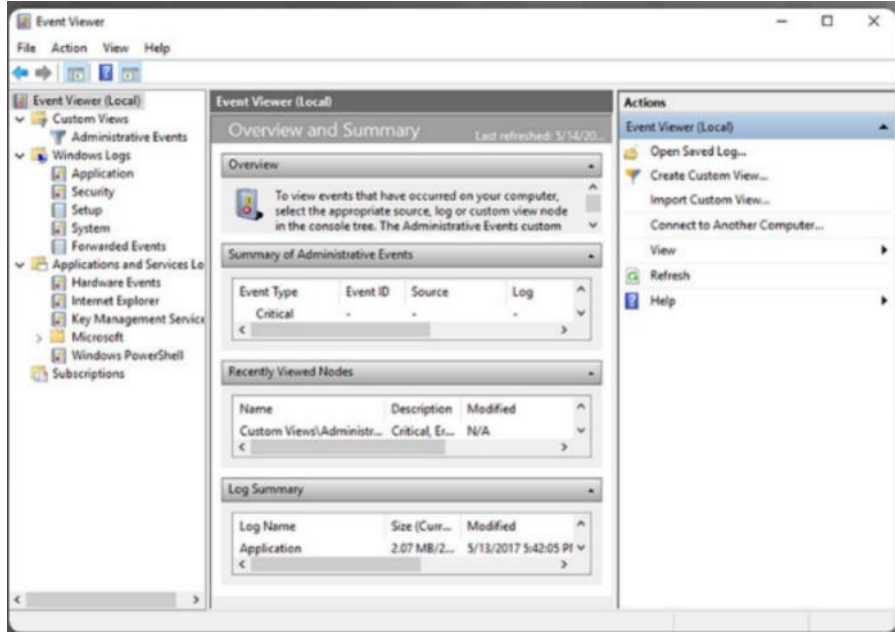
C:\WINDOWS\system32>netstat -abno

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
```

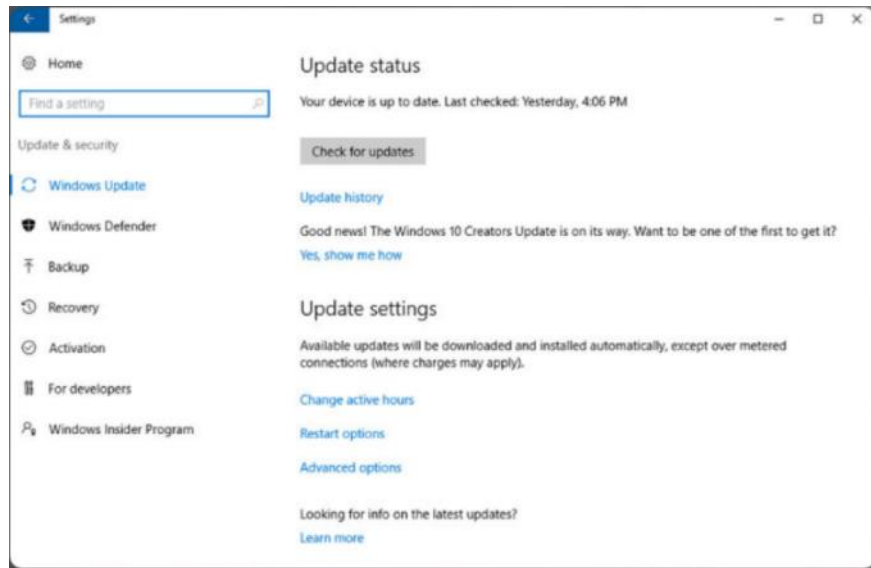
Windows Security

The Event Viewer



- Windows Event Viewer logs the history of application, security, and system events.
- Windows includes two categories of event logs: Windows Logs, and Application and Services Logs.
- A built-in custom view called Administrative Events shows all critical, error, and warning events from all of the administrative logs.

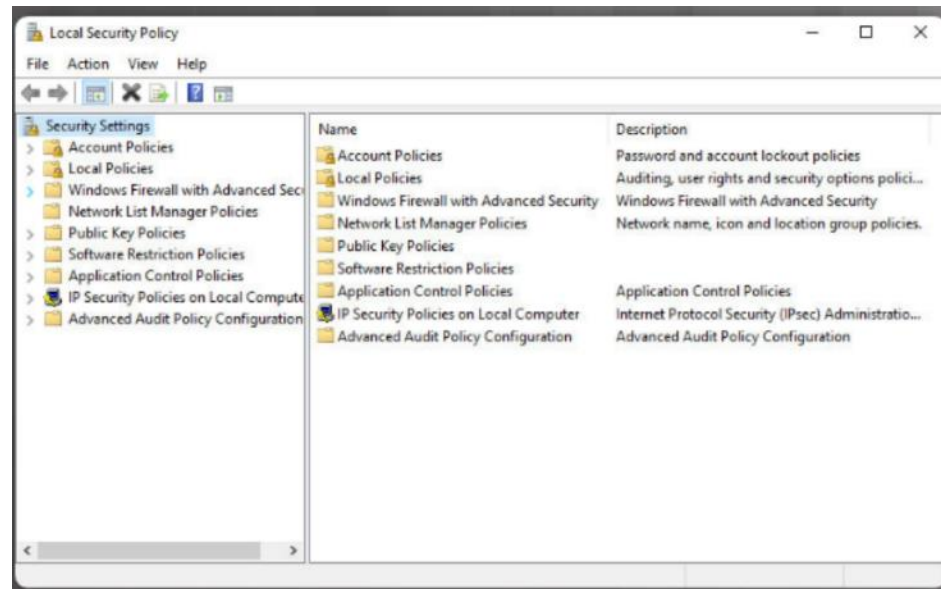
Windows Update Management



- To ensure the highest level of protection against attacks, always make sure Windows is up to date with the latest service packs and security patches.
- Windows routinely checks the Windows Update website for high-priority updates that can help protect a computer from the latest security threats.
- To configure the settings for Windows update, search for Windows Update and click the application.

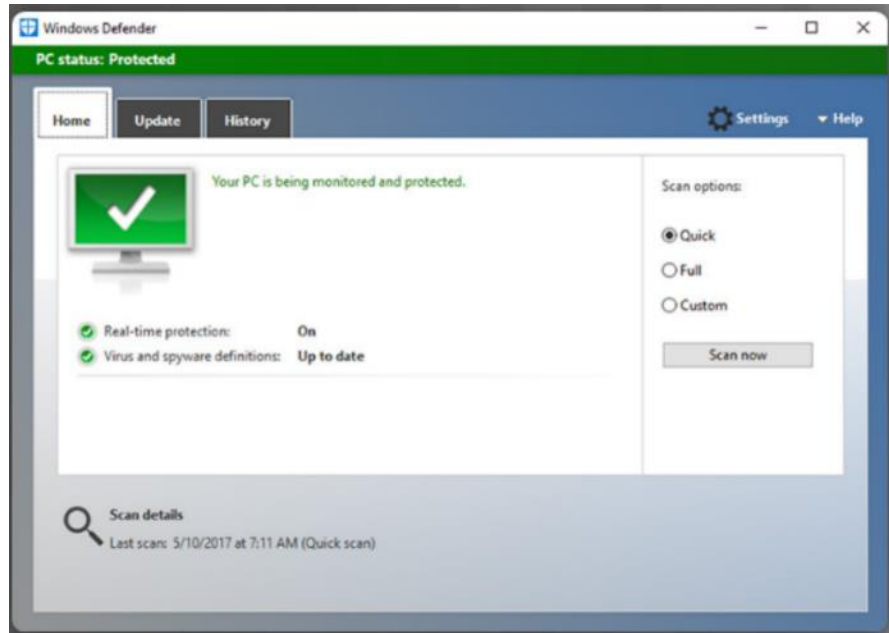
Local Security policy

- Windows Local Security Policy can be used for stand-alone computers that are not part of an Active Directory domain.
- 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 in Account Policies to prevent brute-force login attempts.
- You can also configure User Rights and Firewall Rules.



Windows Security

Local Security policy



- Windows has built-in virus and spyware protection called Windows Defender.
- Windows Defender allows you to perform manual scans of the computer and storage devices, and update the virus and spyware definitions in the Update tab

Windows Security

Windows Firewall

- Firewalls generally work by opening and closing the ports used by various applications.
- Opening only the required ports on a firewall implements a restrictive security policy.
- Most devices now ship with settings as restrictive as possible.

