



institute of  
**continuing**  
education



# Operating Systems Overview

**Md Manirul Islam**

Director, Institute of Continuing Education  
American International University-Bangladesh

# The Windows Operating System



# Windows Overview



# Windows History: Disk Operating System

- Disk Operating System (DOS) is the 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 4006-6939
Directory of C:\

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

# MS-DOS Commands

- The following table lists some of the commands of MS-DOS:

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

# Windows Versions

- Since 1993, there have been more than 20 releases of Windows that are based on the NT operating system.
- 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.
- Microsoft has announced that Windows 10 is the last version of Windows. Rather than purchasing new operating systems, users will just update Windows 10 instead.

OS	Versions
Windows 7	Starter, Home Basic, Home Premium, Professional, Enterprise, Ultimate
Windows Server 2008 R2	Foundation, Standard, Enterprise, Data Center, Web Server, HPC Server, Itanium-Based Systems
Windows 8	Windows 8, Windows 8 Pro, Windows 8 Enterprise, Windows RT
Windows Server 2012	Foundation, Essentials, Standard, Data Center
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, Data Center
Windows 10	Home, Pro, Pro Education, Enterprise, Education, IoT Core, Mobile, Mobile Enterprise
Windows Server 2016	Essentials, Standard, Datacenter, Multipoint Premium Server, Storage Server, Hyper-V Server

# Windows GUI

- Windows has a graphical user interface (GUI) for users to work with data files and software.
- The GUI has a main area that is known as the Desktop. The Desktop can be customized with various colors and background images.
- Windows supports multiple users, so each user can customize the Desktop.
- The Desktop can store files, folders, shortcuts to locations and programs, and applications.
- Windows File Explorer, is a tool used to navigate the entire file system of a computer.



# Windows Architecture: Hardware Abstraction Layer

- A hardware abstraction layer (HAL) is software 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.

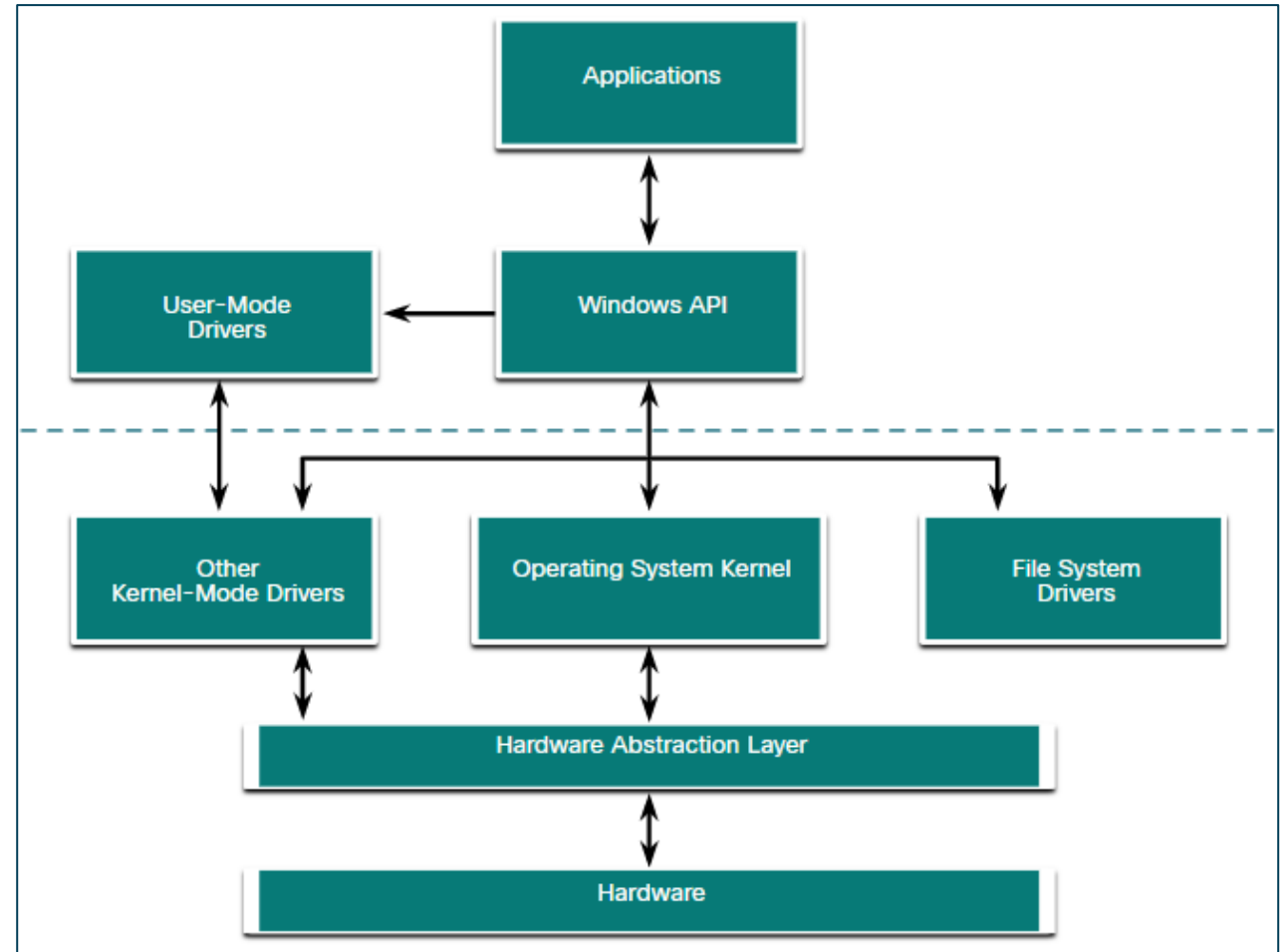
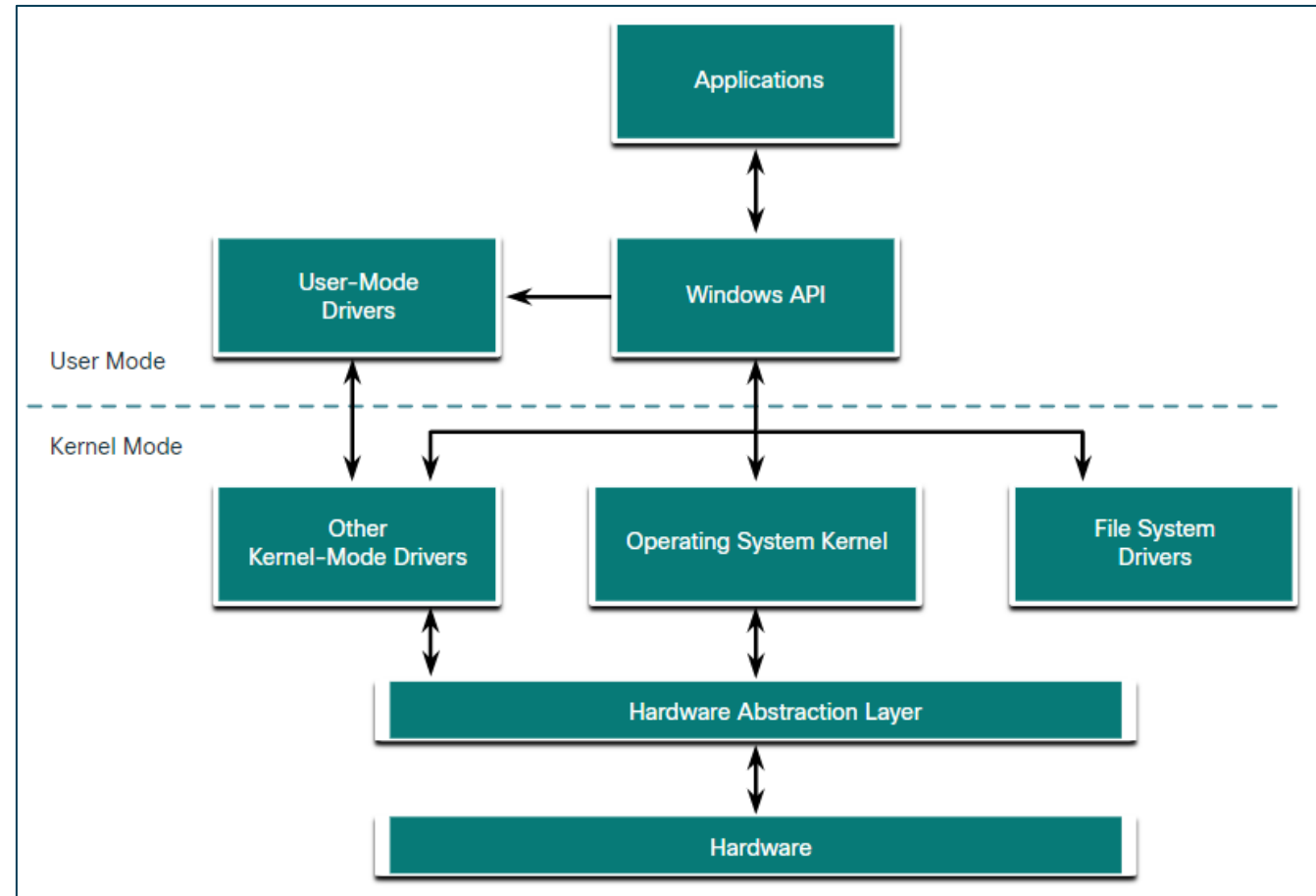


Figure: Basic Windows Architecture



# Windows Architecture: 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.
- All of the code that runs in kernel mode uses the same address space.
- 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.

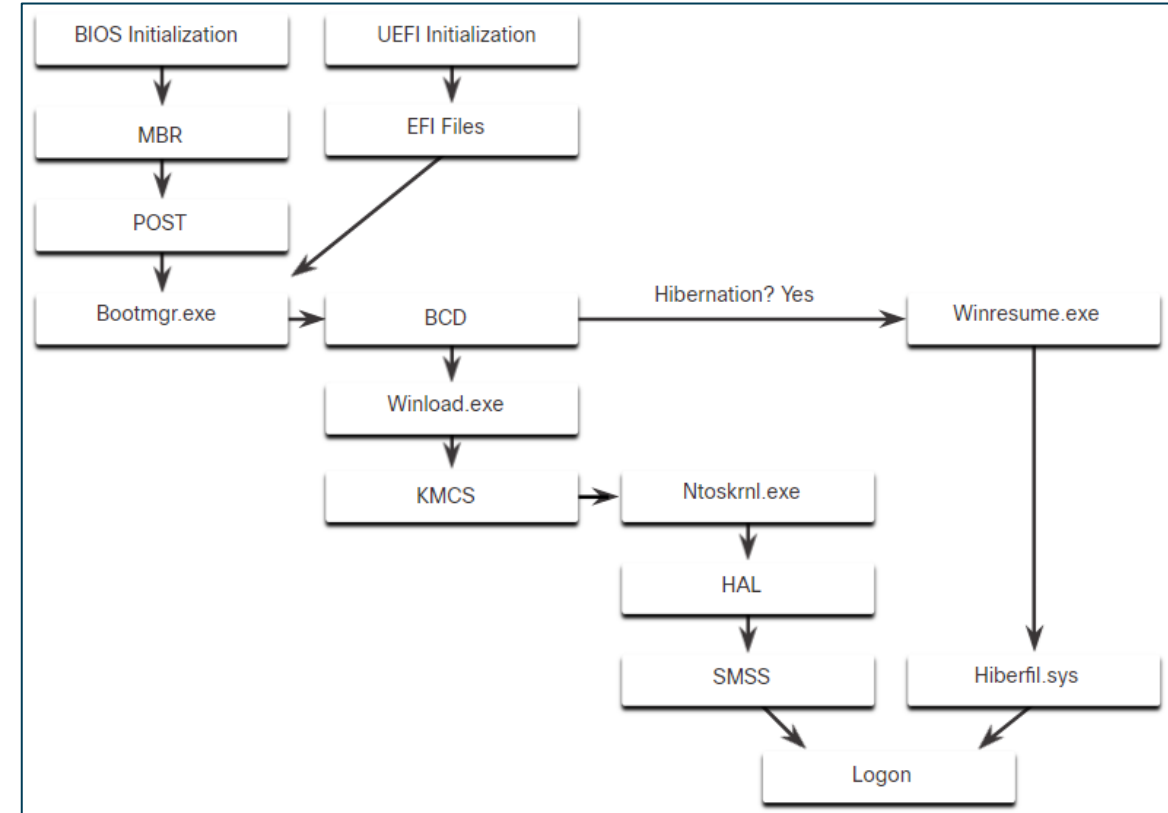


# Windows File Systems

- A file system is a way of organizing the information 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.

# Windows Boot Process

- Many actions occur between the power button is pressed and Windows is fully loaded. This is the Windows Boot process. Two types of computer firmware exist:
  - Basic Input-Output System (BIOS):** The process begins with the BIOS initialization phase in which the hardware devices are initialized and a POST is performed. When the system disk is discovered, the POST ends and looks for the master boot record (MBR). The BIOS executes the MBR code and the operating system starts to load.
  - Unified Extensible Firmware Interface (UEFI):** UEFI firmware boots by loading EFI program files (.efi) stored in a special disk partition, known as the EFI System Partition (ESP).

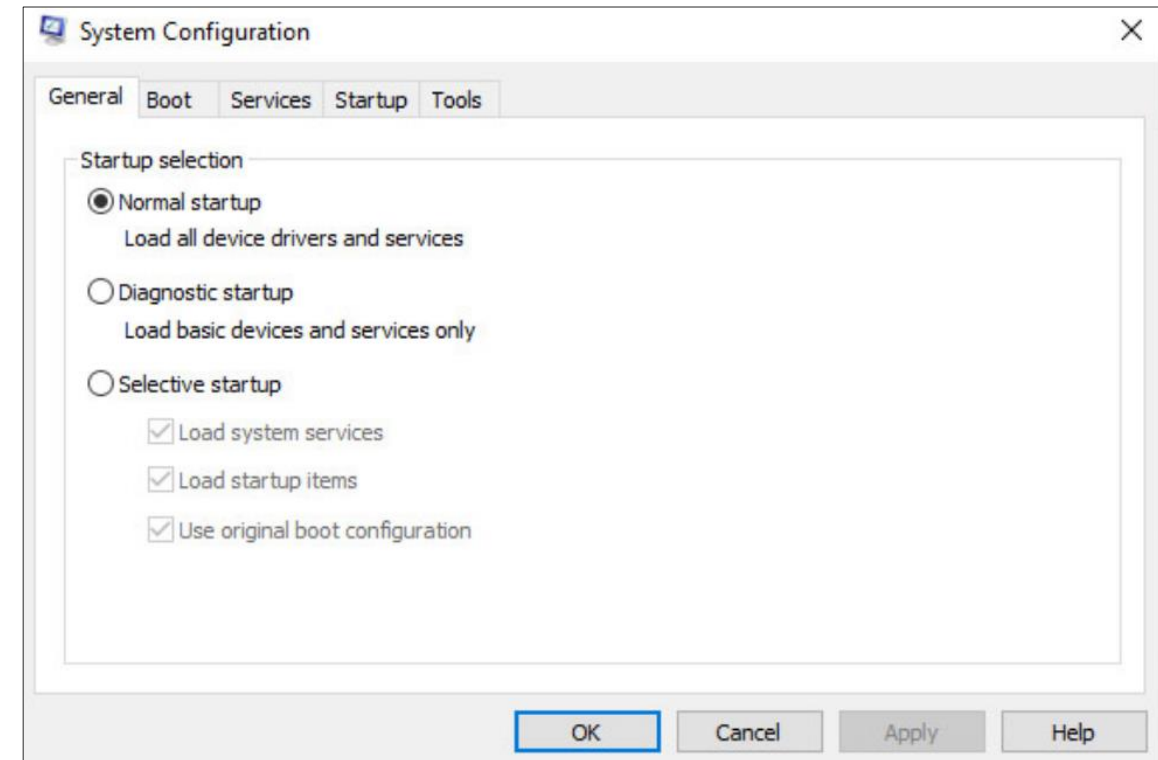


# Windows Boot Process

- Whether the firmware is BIOS or UEFI, after a valid Windows installation is located, the Bootmgr.exe file is run.
- Bootmgr.exe reads the Boot Configuration Database (BCD).
- If the computer is coming out of hibernation, the boot process continues with Winresume.exe.
- If the computer is being booted from a cold start, then the Winload.exe file is loaded.
- Winload.exe also uses Kernel Mode Code Signing (KMCS) to make sure that all drivers are digitally signed.
- After the drivers have been examined, Winload.exe runs Ntoskrnl.exe that starts the Windows kernel and sets up the HAL.

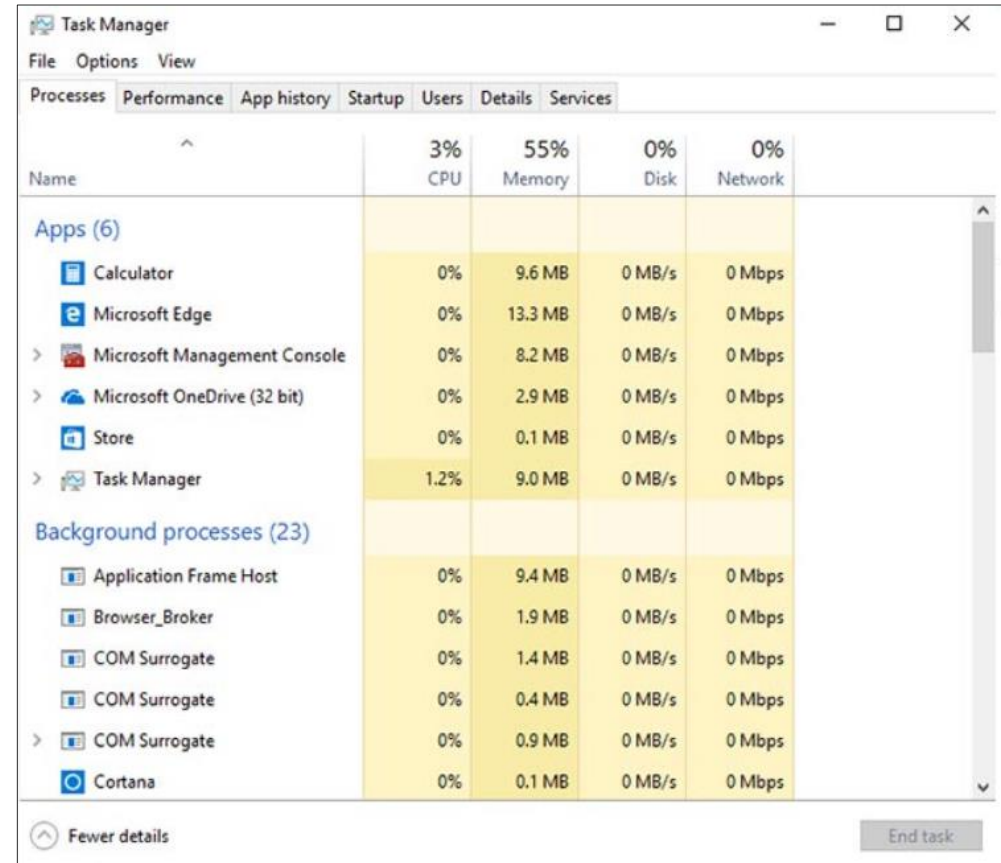
# Windows Startup and Shutdown

- There are two important registry items that are used to automatically start applications and services:
  - HKEY\_LOCAL\_MACHINE
  - HKEY\_CURRENT\_USER
- 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.
- It is always best to perform a proper shutdown to turn off the computer.



# Processes, Threads, and Services

- A Windows application is made up of processes. 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.
- 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.
- To configure Windows processes, search for Task Manager. The Processes tab of the Task Manager is shown in the figure.



Task Manager

File Options View

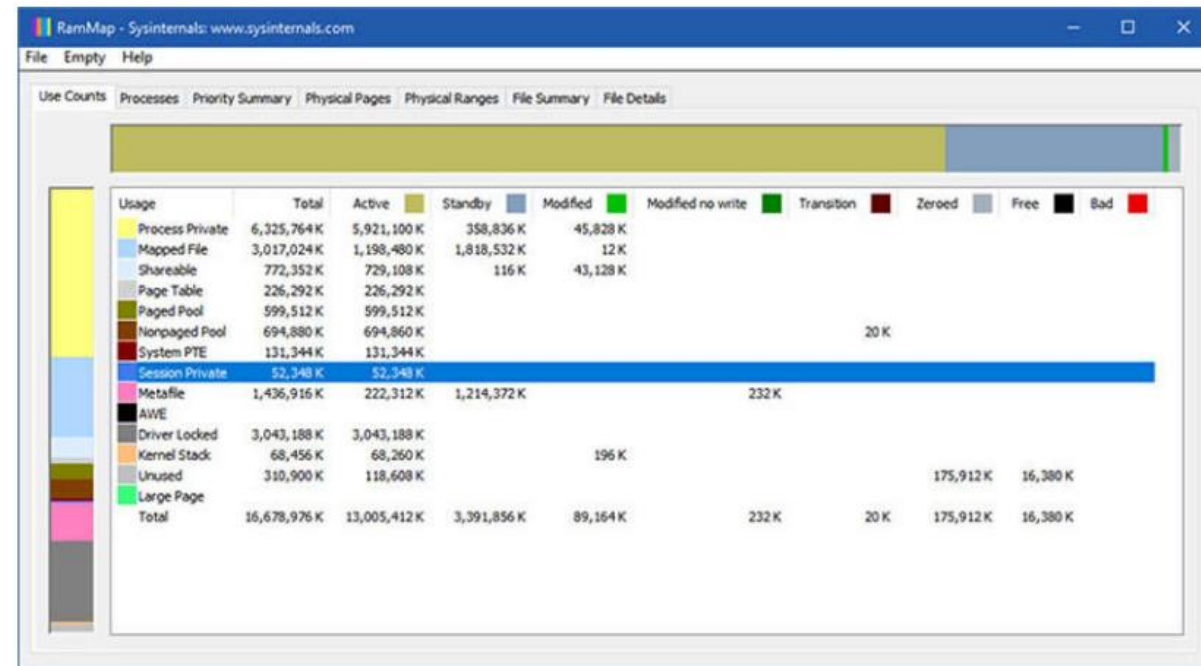
Processes Performance App history Startup Users Details Services

Name	3% CPU	55% Memory	0% Disk	0% Network
<strong>Apps (6)</strong>				
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
<strong>Background processes (23)</strong>				
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

^ Fewer details End task

# 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.
- Sysinternal's RamMap – Used to view memory allocation.



# The Windows Registry

- 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, below that there are keys, followed by subkeys.
- Values store data and are stored in the keys and subkeys. A registry key can be up to 512 levels deep.
- The following table lists the five hives of the Windows registry:

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

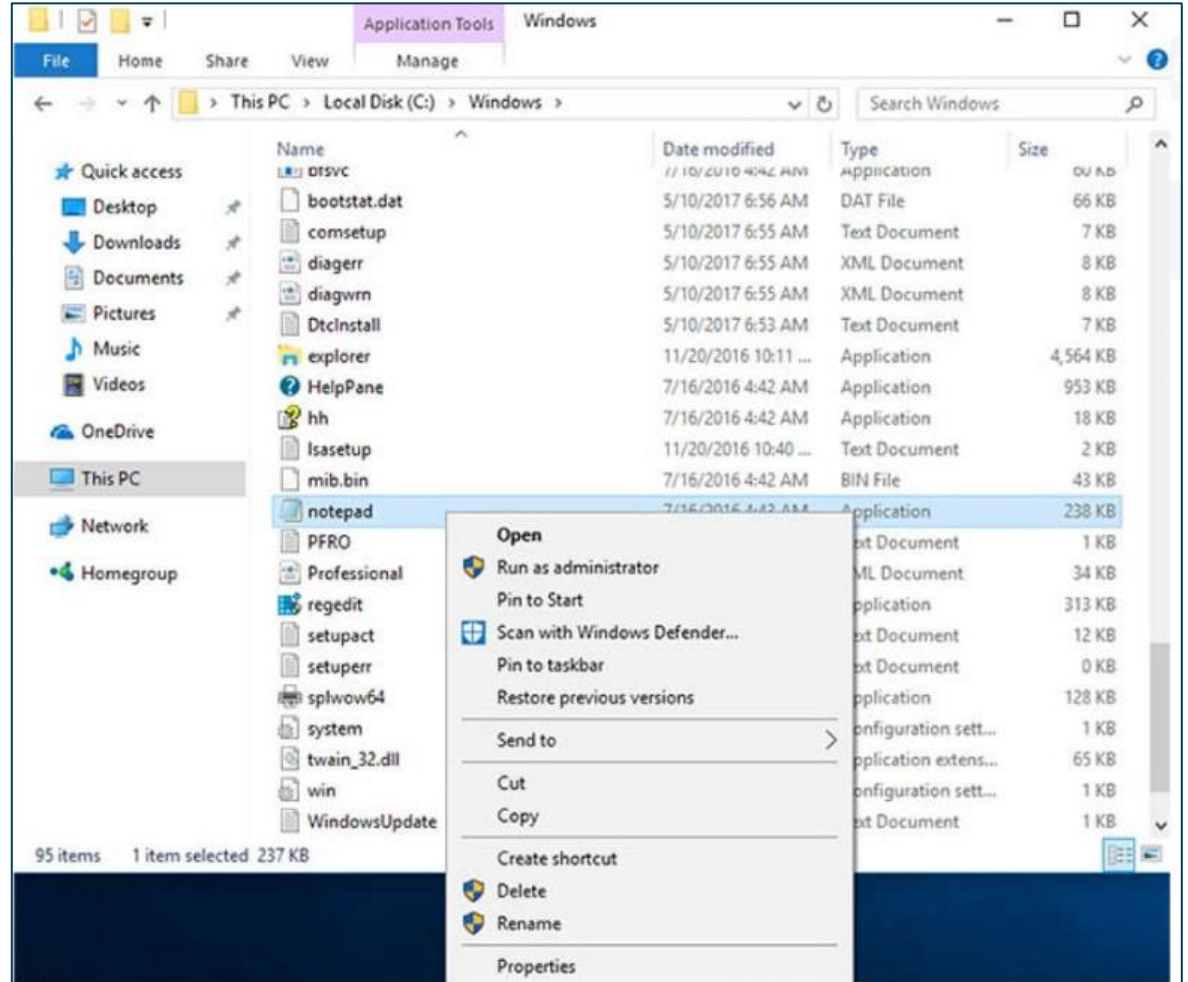


# Windows Administration



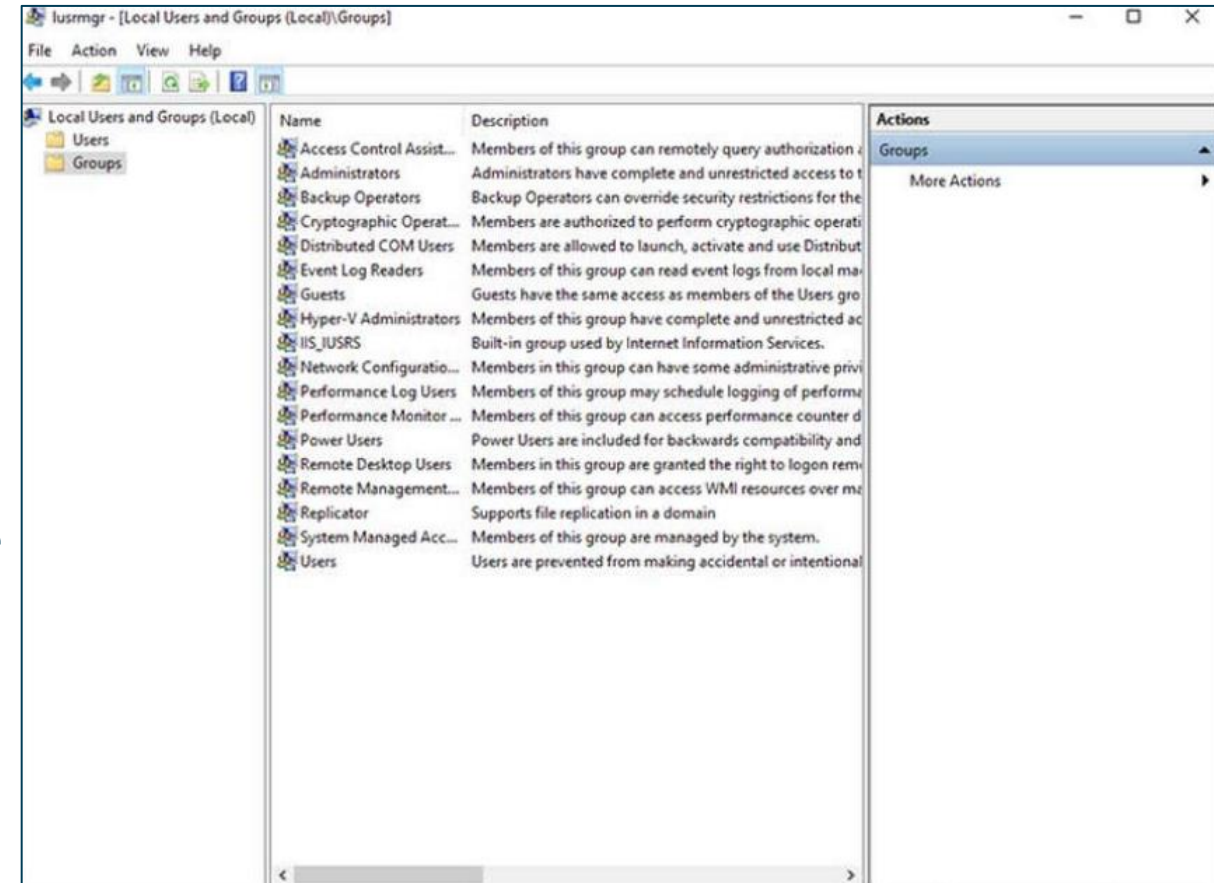
# Run as Administrator

- As a security best practice, it is not advisable to log on to Windows using the Administrator account or an account with administrative privileges.
- Sometimes, it is necessary to run or install software that requires the privileges of the Administrator.
- Right-click the command in the Windows File Explorer and choose Run as Administrator from the Context Menu or open an Administrator Command Prompt.



# 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).



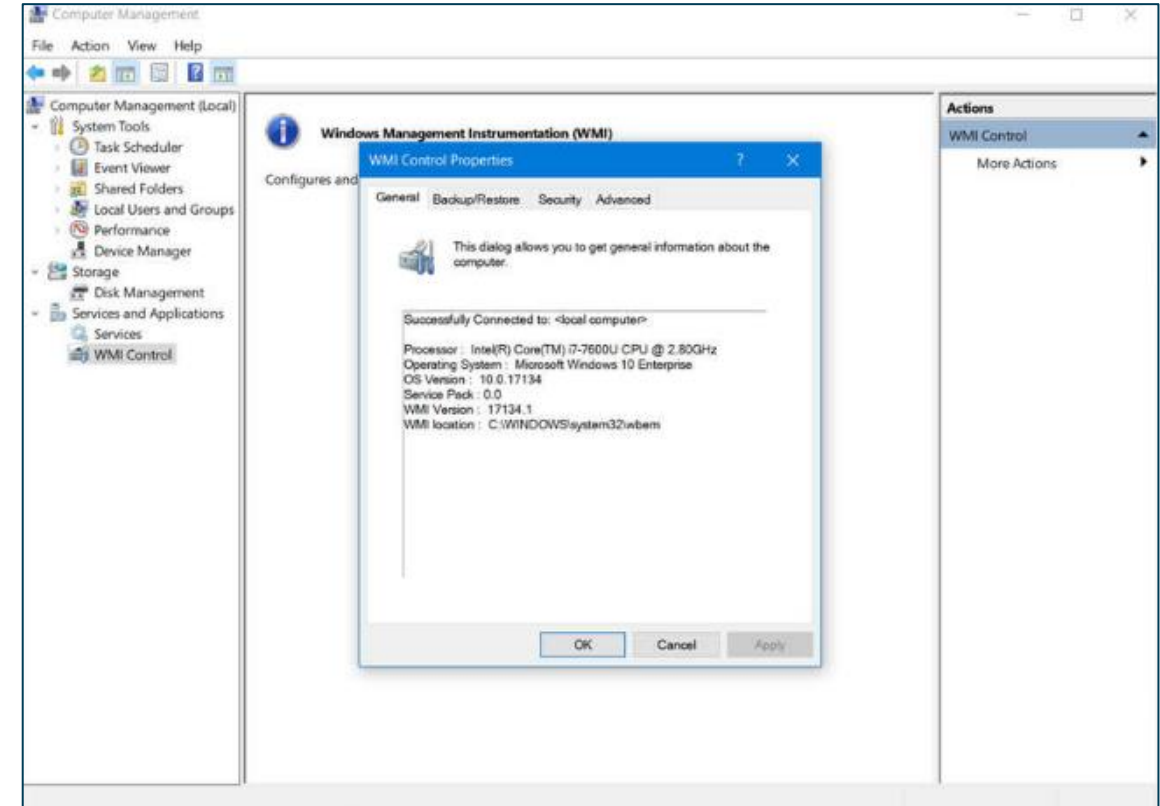
# CLI and Powershell

- 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.
- 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.

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

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



# The net Command

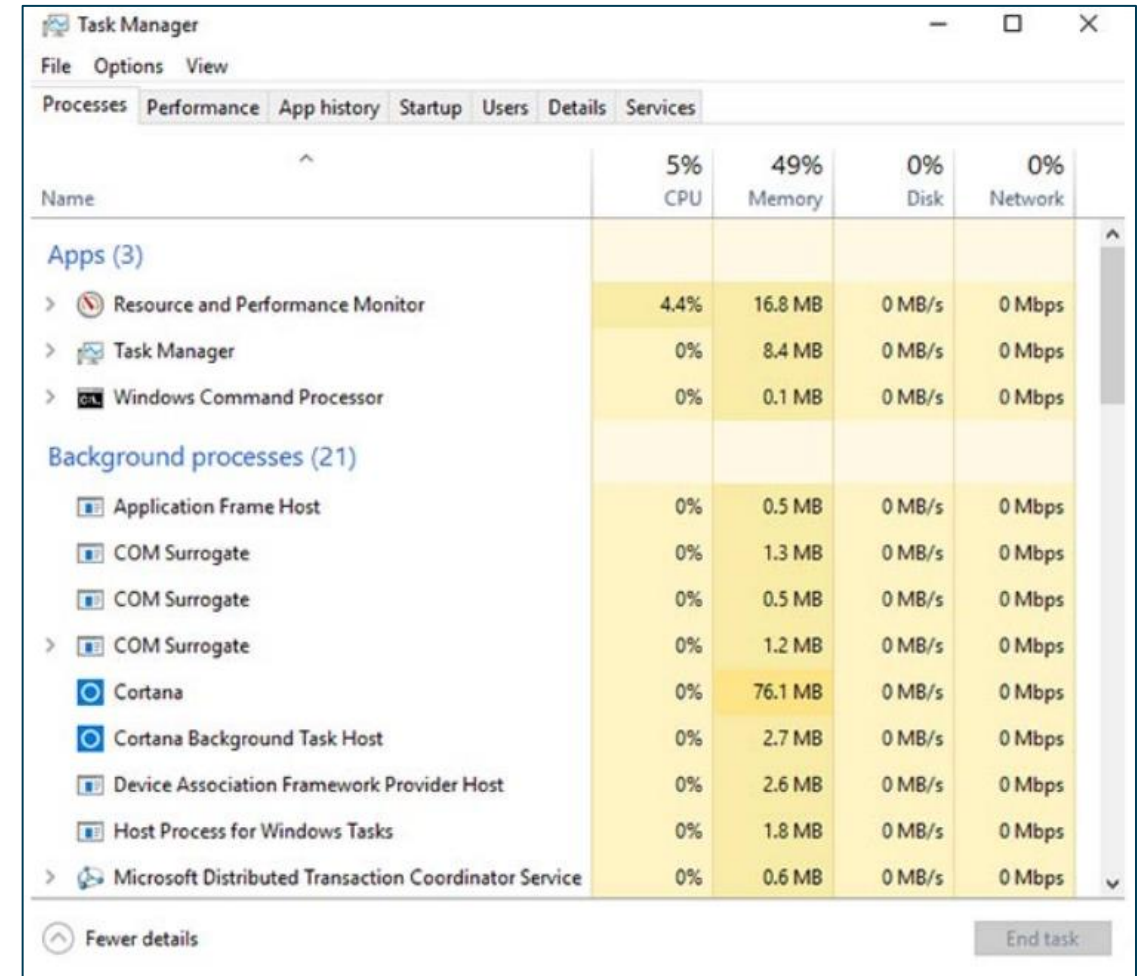
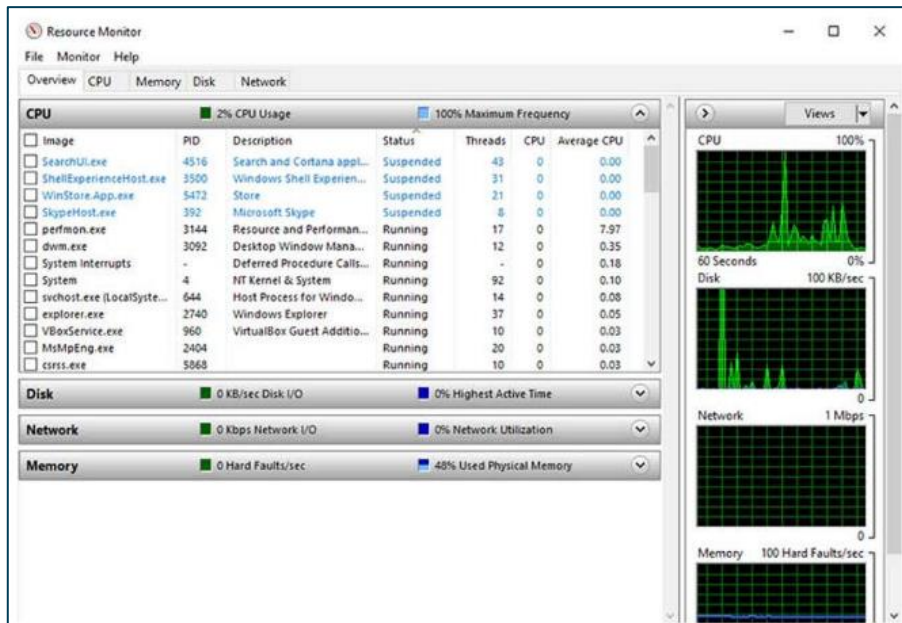
- The net command is used in the administration and maintenance of the OS.
- The net command supports many subcommands that follow it and can be combined with switches to focus on specific output.
- To see a list of the many net commands, type net help at the command prompt.
- The command output shows the commands that the net command can use.
- To see verbose help about any of the net commands, type C:\> net help.

```
C:\> net help
The syntax of this command is:
NET HELP
command
    -or-
NET command /HELP
Commands available are:
NET ACCOUNTS          NET HELPMMSG          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:\>
```



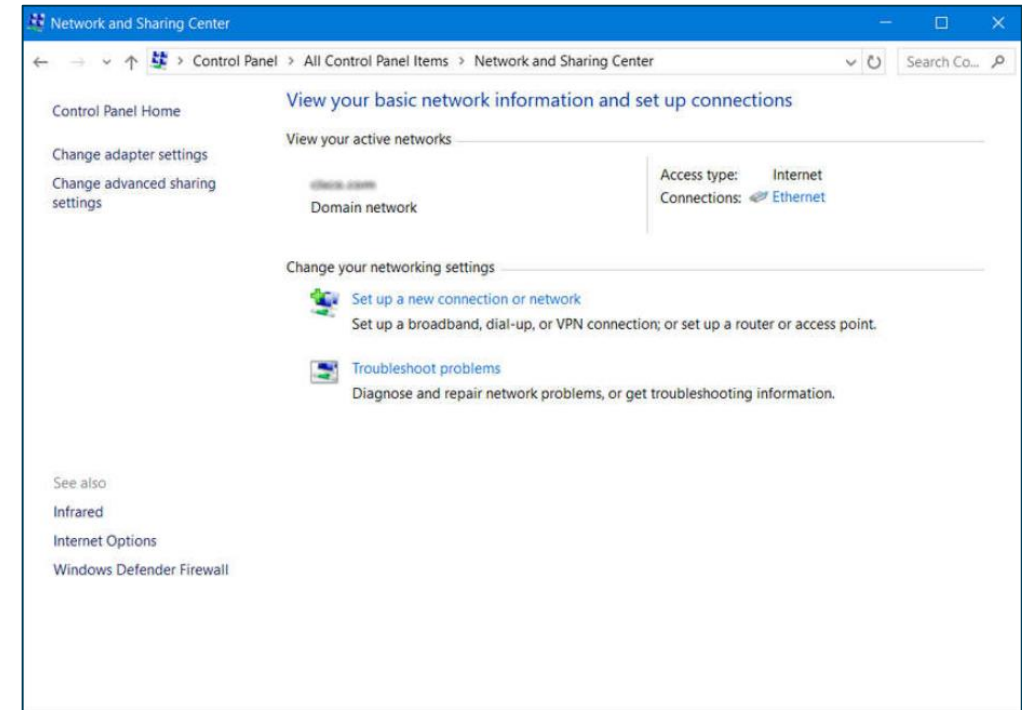
# Task Manager and Resource Monitor

- 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.



# Networking

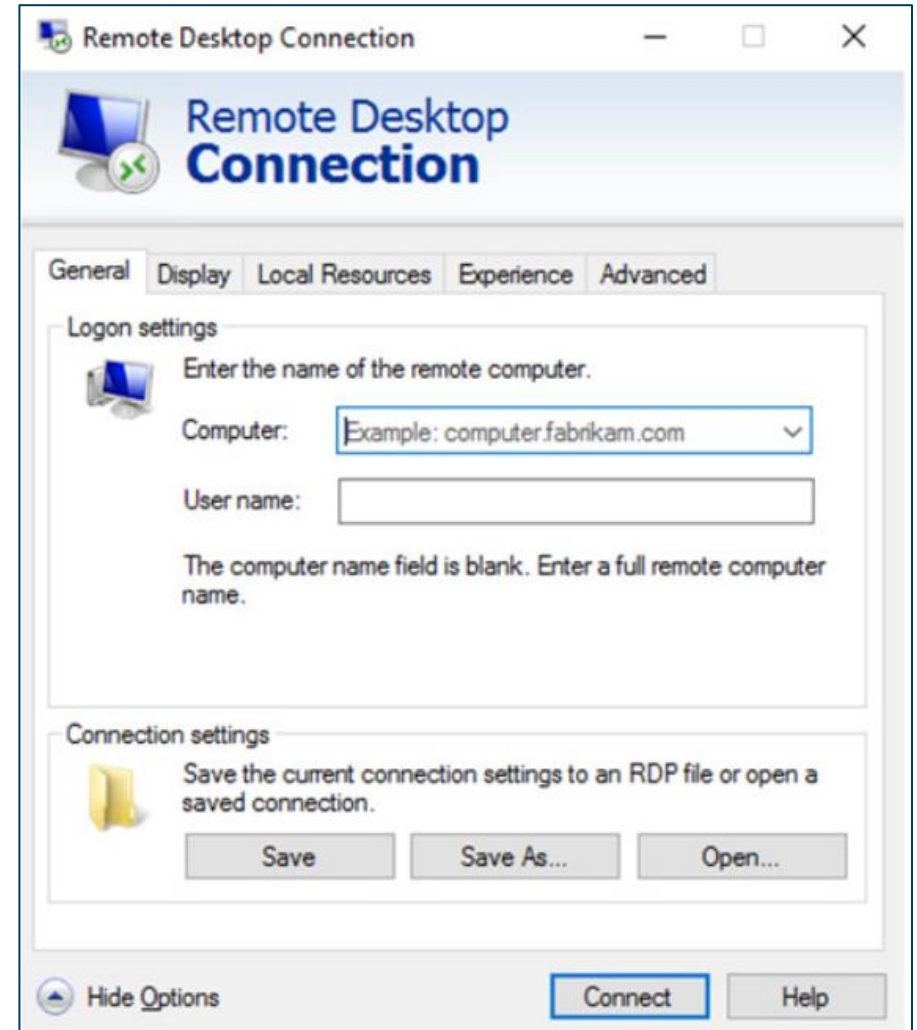
- One of the most important features of any operating system is the ability for the computer to connect to a network.
- To configure Windows networking properties and test networking settings, the Network and Sharing Center is used.
- Use the **netsh.exe** tool to configure networking parameters from 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.





# Accessing Network Resources

- Server Message Block (SMB) protocol is used to share network resources. It is mostly used for accessing files on remote hosts.
- The Universal Naming Convention (UNC) format is used to connect to resources such as **\\servername\sharename\file**
- An administrative share automatically created by Windows 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 Server

- Most Windows installations are performed as desktop installations on desktops and laptops.
- There is another edition of Windows that is mainly used in data centers called Windows Server. This is a family of Microsoft products that began with Windows Server 2003.
- Windows Server hosts many different services and can fulfill different roles within a company.
- These are some of the services that Windows Server provides:
  - **Network Services:** DNS, DHCP, Terminal services, Network Controller, and Hyper-V Network virtualization
  - **File Services:** SMB, NFS, and DFS
  - **Web Services:** FTP, HTTP, and HTTPS
  - **Management:** Group policy and Active Directory domain services control

# Windows Security



# The netstat Command

- The **netstat** command is used to look for inbound or outbound connections that are not authorized.

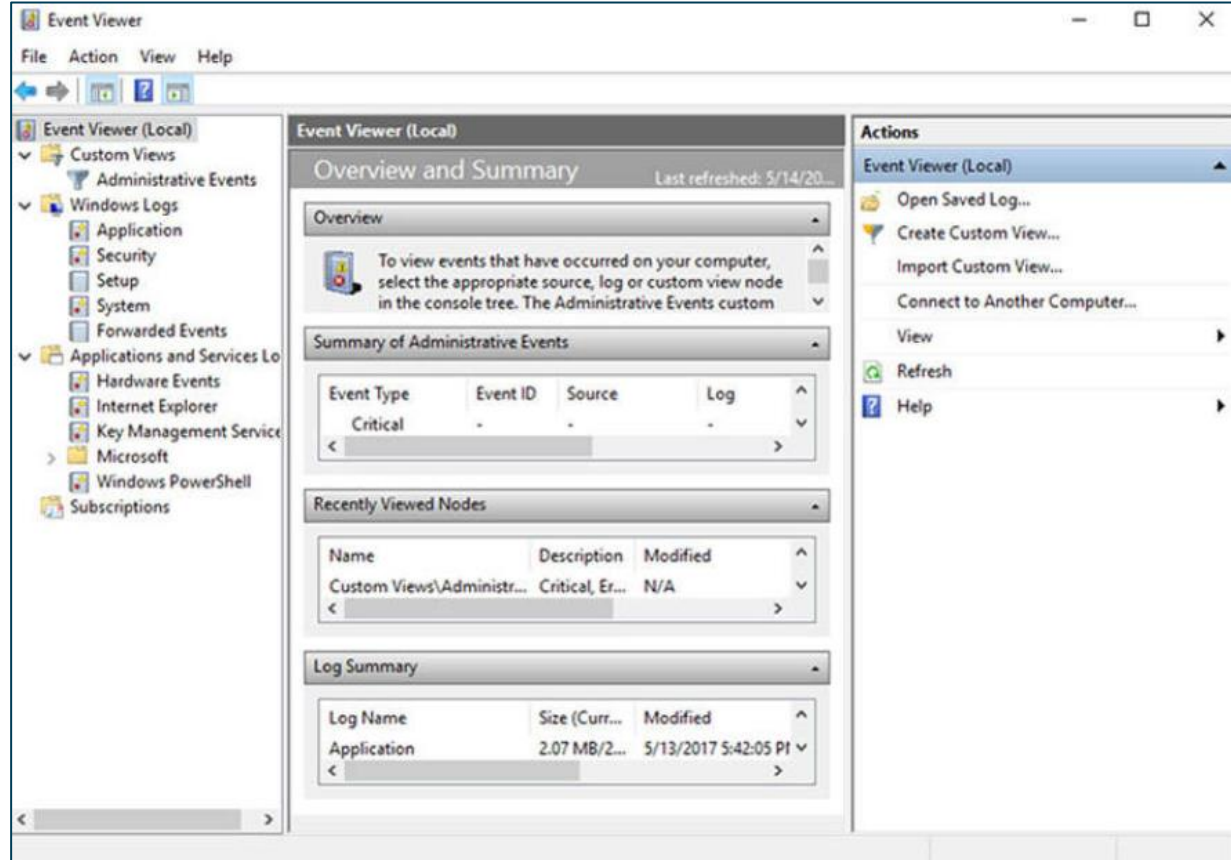
The **netstat** command will display all of the active TCP connections.

- 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**.

```
Microsoft Windows [Version 10.0.18363.720]
(c) 2019 Microsoft Corporation. All rights reserved.
C:\WINDOWS\system32> netstat -abno
Active Connections
  Proto Local Address           Foreign Address         State       PID
  TCP    0.0.0.0:80               0.0.0.0:0               LISTENING   4
Can not obtain ownership information
  TCP    0.0.0.0:135              0.0.0.0:0               LISTENING   952
RpcSs
[svchost.exe]
  TCP    0.0.0.0:445              0.0.0.0:0               LISTENING   4
Can not obtain ownership information
  TCP    0.0.0.0:623              0.0.0.0:0               LISTENING   14660
[LMS.exe]
  TCP    0.0.0.0:3389             0.0.0.0:0               LISTENING   1396
TermService
[svchost.exe]
  TCP    0.0.0.0:5040             0.0.0.0:0               LISTENING   9792
CDPSvc
[svchost.exe]
  TCP    0.0.0.0:5357             0.0.0.0:0               LISTENING   4
Can not obtain ownership information
  TCP    0.0.0.0:5593             0.0.0.0:0               LISTENING   4
Can not obtain ownership information
  TCP    0.0.0.0:8099             0.0.0.0:0               LISTENING   5248
[SolarWinds TFTP Server.exe]
  TCP    0.0.0.0:16992            0.0.0.0:0               LISTENING   14660
```

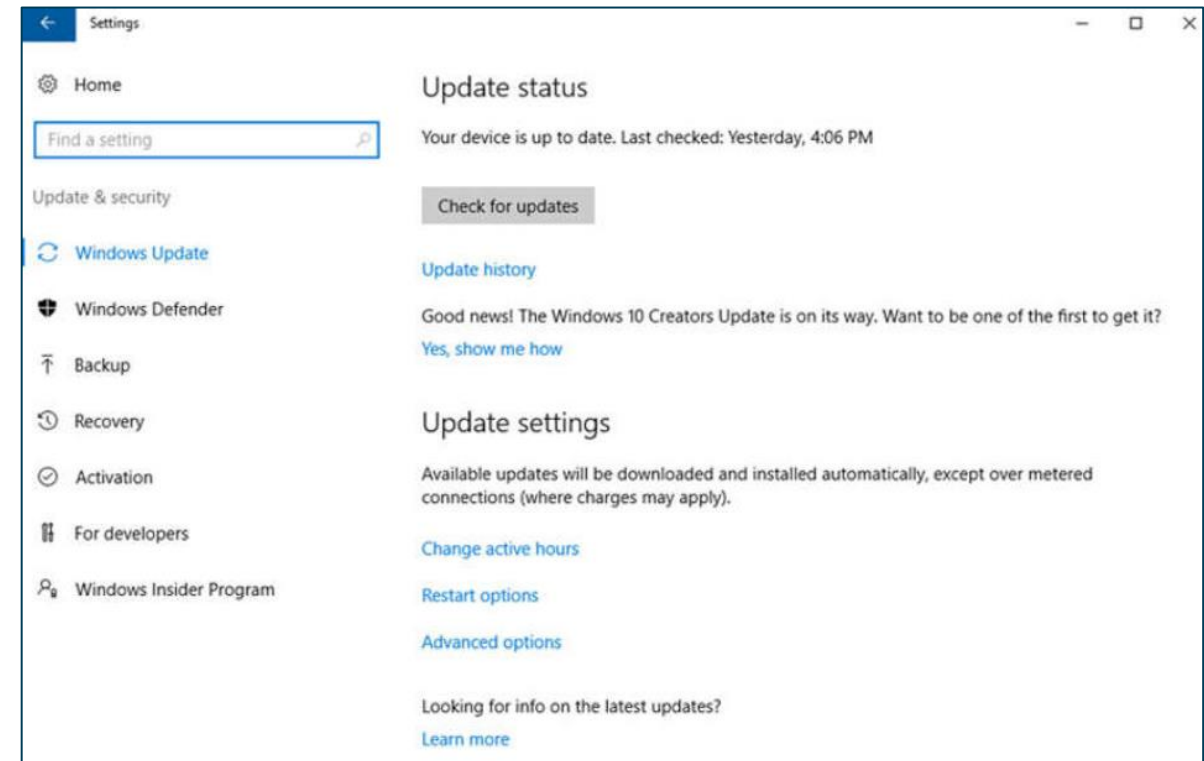
# The Event Viewer

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



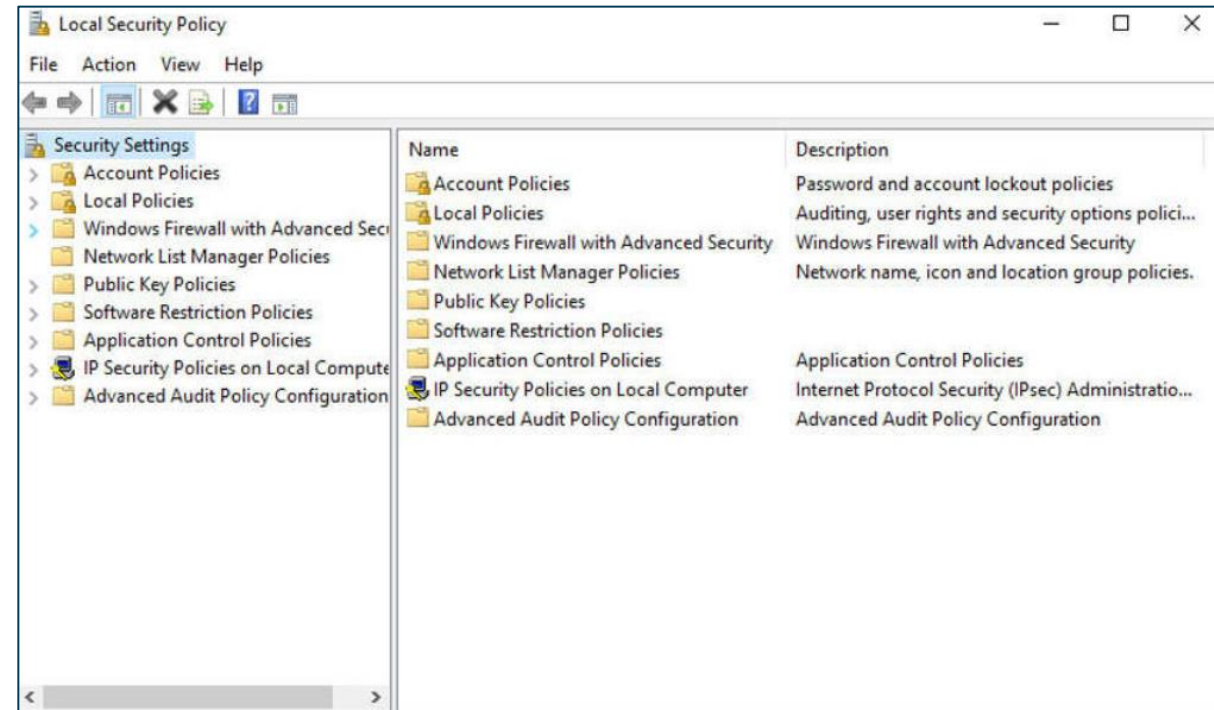
# Windows Update Management

- 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.
- 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.



# Local Security Policy

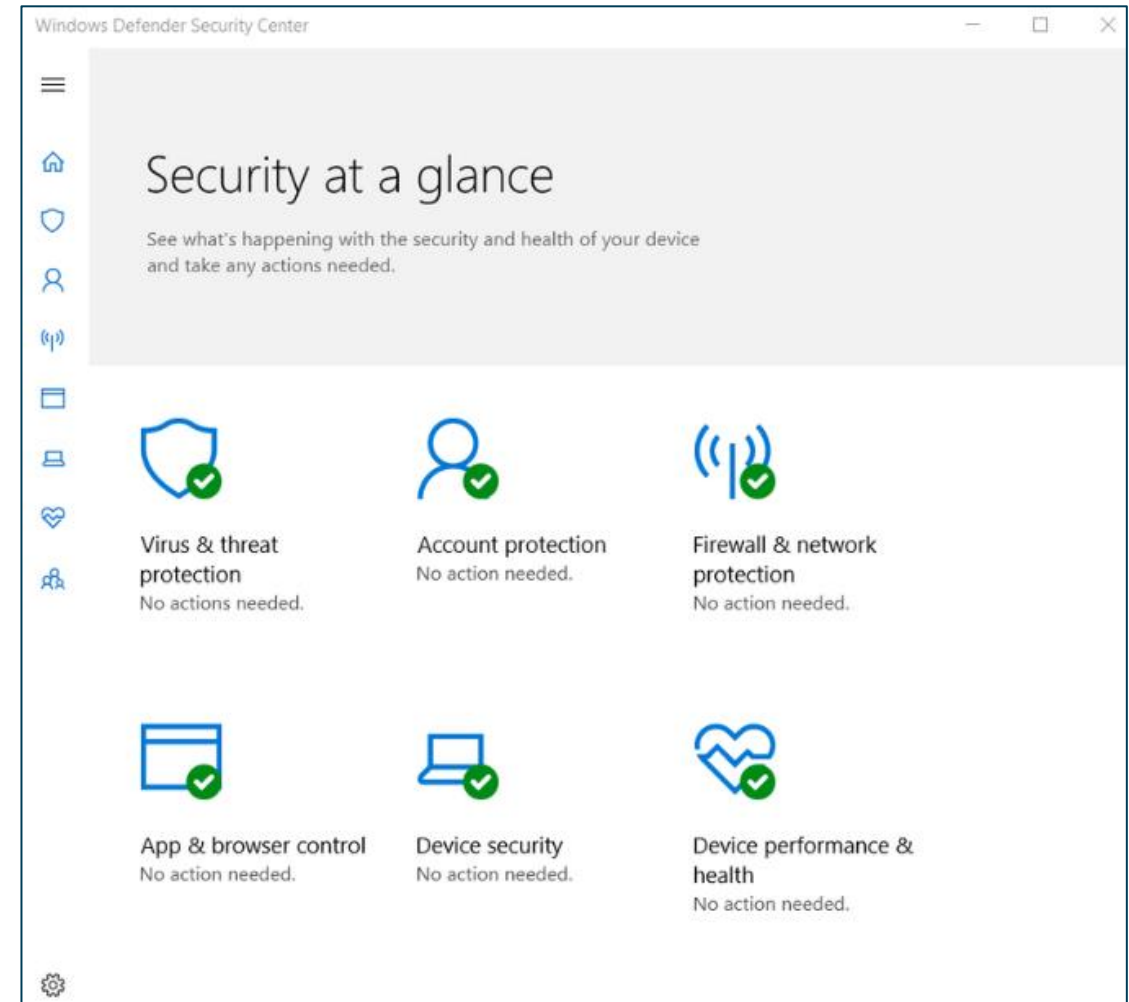
- Windows Local Security Policy can be used for stand-alone computers that are not part of an Active Directory domain.
- Password Policy is found under Account Policies and defines the criteria for the passwords for all of the users on the local computer.
- Use the Account Lockout Policy in Account Policies to prevent brute-force login attempts.
- You can also configure User Rights and Firewall Rules.





# Windows Defender

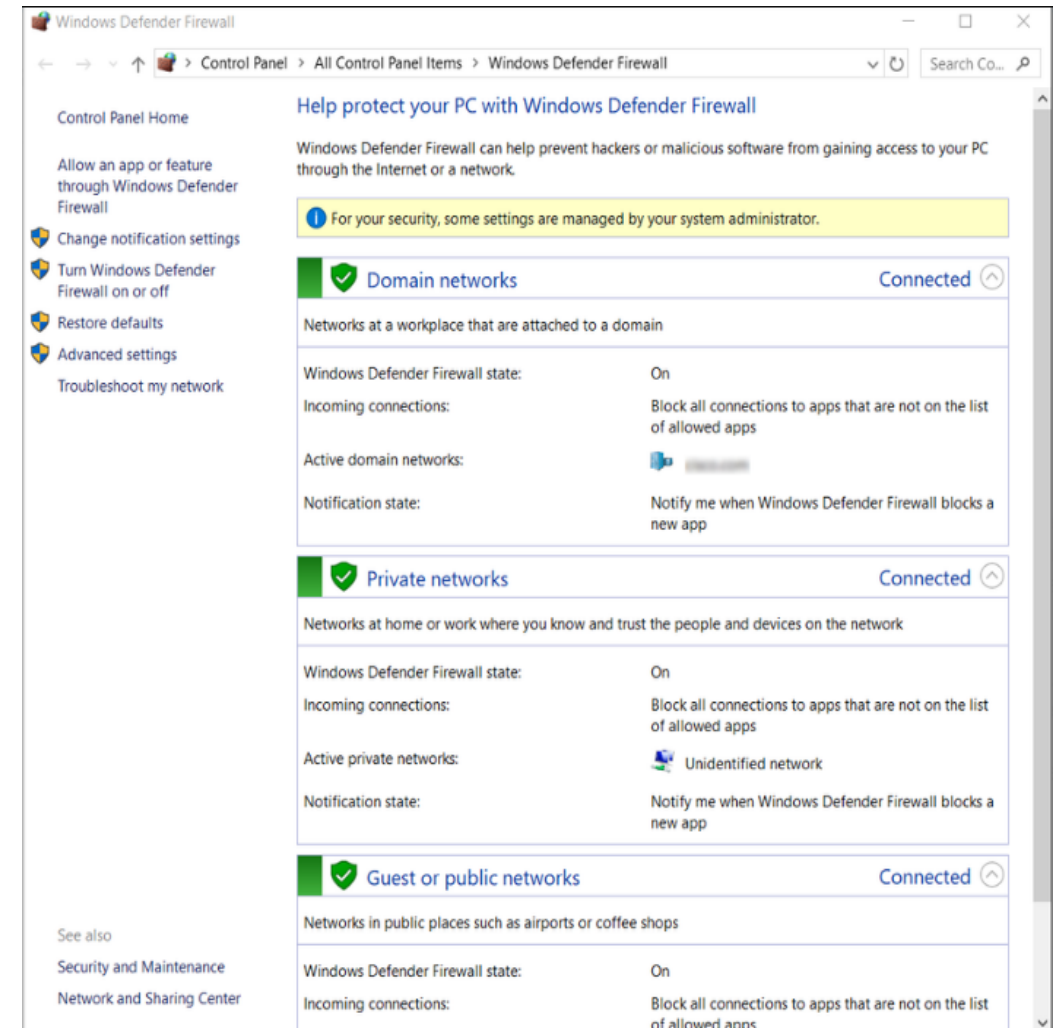
- It is important to protect computers and mobile devices using reputable antimalware software. Windows has built-in virus and spyware protection called Windows Defender.
- Windows Defender is turned on by default to provide real-time protection against infection.
- Although Windows Defender works in the background, the user can perform manual scans of the computer and storage devices.
- Several security organizations such as McAfee, Symantec, and Kaspersky offer all-inclusive malware protection for computers and mobile devices.





# Windows Defender Firewall

- A firewall selectively denies traffic to a computer or network segment.
- To allow program access through the Windows Defender Firewall, search for **Control Panels**. Under **Systems and Security**, locate **Windows Defender Firewall**. Click **Allow an app or feature through Windows Defender Firewall**, as shown in the figure.
- To disable the Windows Firewall and use a different software firewall, click **Turn Windows Firewall on or off**.
- Many additional settings can be found under **Advanced settings**. Here, inbound or outbound traffic rules can be created, and different aspects of the firewall can be monitored.



# Linux Operating System

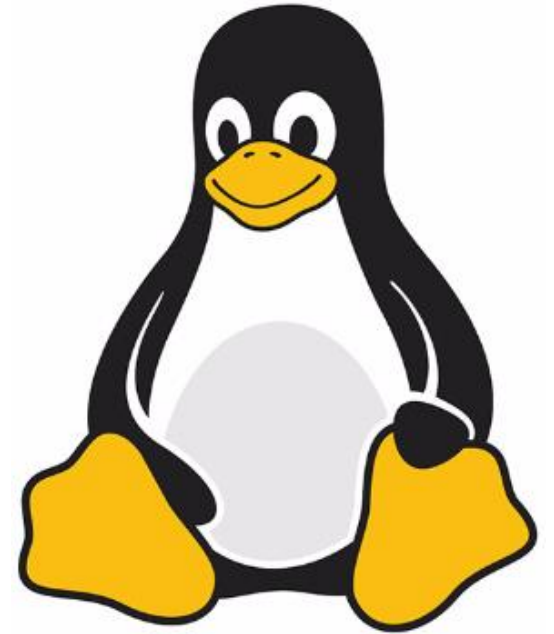


# Linux Basics



# What is Linux?

- Linux is an operating system that was created in 1991.
- Linux is open source, fast, reliable, and small. It requires very little hardware resources to run and is highly customizable.
- Linux is part of several platforms and can be found on devices anywhere from wristwatches to supercomputers.
- Linux is designed to be connected to the network, which makes it much simpler to write and use network-based applications.
- A Linux distribution is the term used to describe packages created by different organizations and include the Linux kernel with customized tools and software packages.

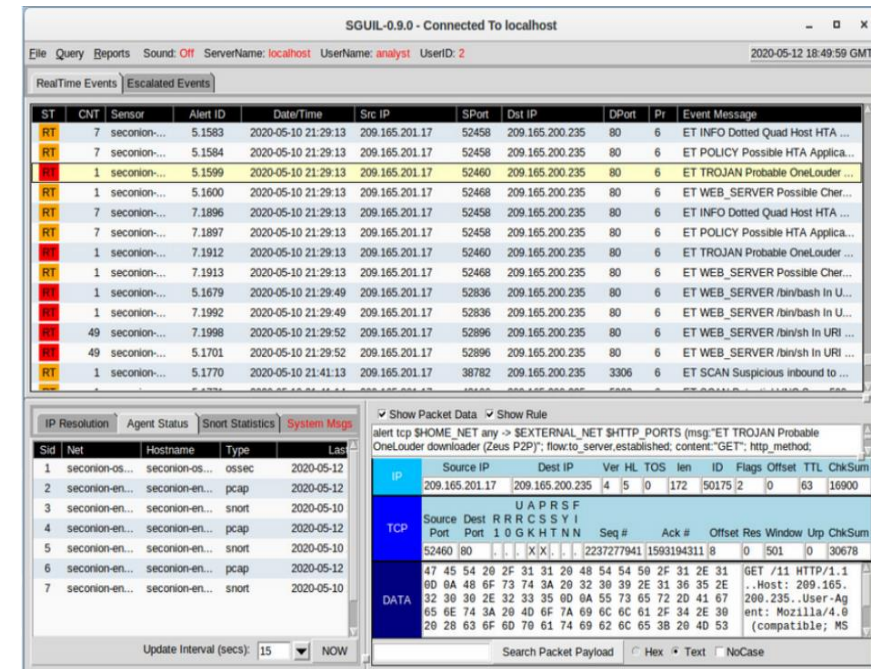


# The Value of Linux

- Linux is often the operating system of choice in the Security Operations Center (SOC). These are some of the reasons to choose Linux:
  - **Linux is open source** - Any person can acquire Linux at no charge and modify it to fit specific needs.
  - **The Linux CLI is very powerful** - The Linux Command Line Interface (CLI) is extremely powerful and enables analysts to perform tasks not only directly on a terminal, but also remotely.
  - **The user has more control over the OS** - The administrator user in Linux, known as the root user, or superuser, can modify any aspect of the computer with a few keystrokes.
  - **It allows for better network communication control** - Control is an inherent part of Linux.

# Linux in the SOC

- The flexibility provided by Linux is a great feature for the SOC. The entire operating system can be tailored to become the perfect security analysis platform.
- Security Onion is an open-source suite of tools that work together for network security analysis.
- The following are few tools that are often found in a SOC:
  - Network Packet Capture Software (Wireshark)
  - Malware Analysis Tools
  - Intrusion Detection Systems (IDSs)
  - Firewalls
  - Log Managers
  - Security Information and Event Management (SIEM)
  - Ticketing Systems



# Linux Tools

- Linux computers that are used in the SOC often contain penetration testing tools.
- A penetration test, also known as PenTesting, is the process of looking for vulnerabilities in a network or computer by attacking it.
- Packet generators, port scanners, and proof-of-concept exploits are examples of PenTesting tools.
- Kali Linux is a Linux distribution which contains many penetration tools together in a single Linux distribution.
- Notice all the major categories of penetration testing tools of Kali Linux.



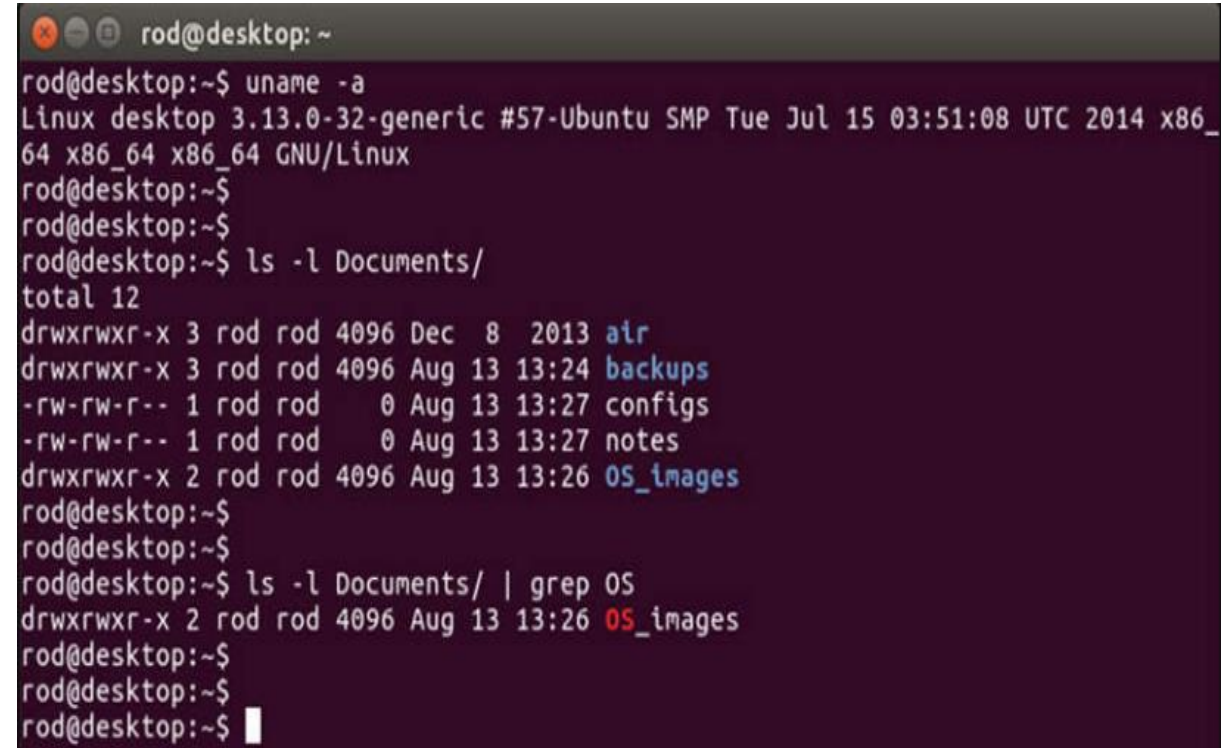
# Working in the Linux Shell





# The Linux Shell

- In Linux, the user communicates with the OS by using the CLI or the GUI.
- Terminal emulator applications provide user access to the CLI.
- Popular terminal emulators are Terminator, eterm, xterm, konsole, and gnome-terminal.
- Fabrice Bellard has created JSLinux which allows an emulated version of Linux to run in a browser.



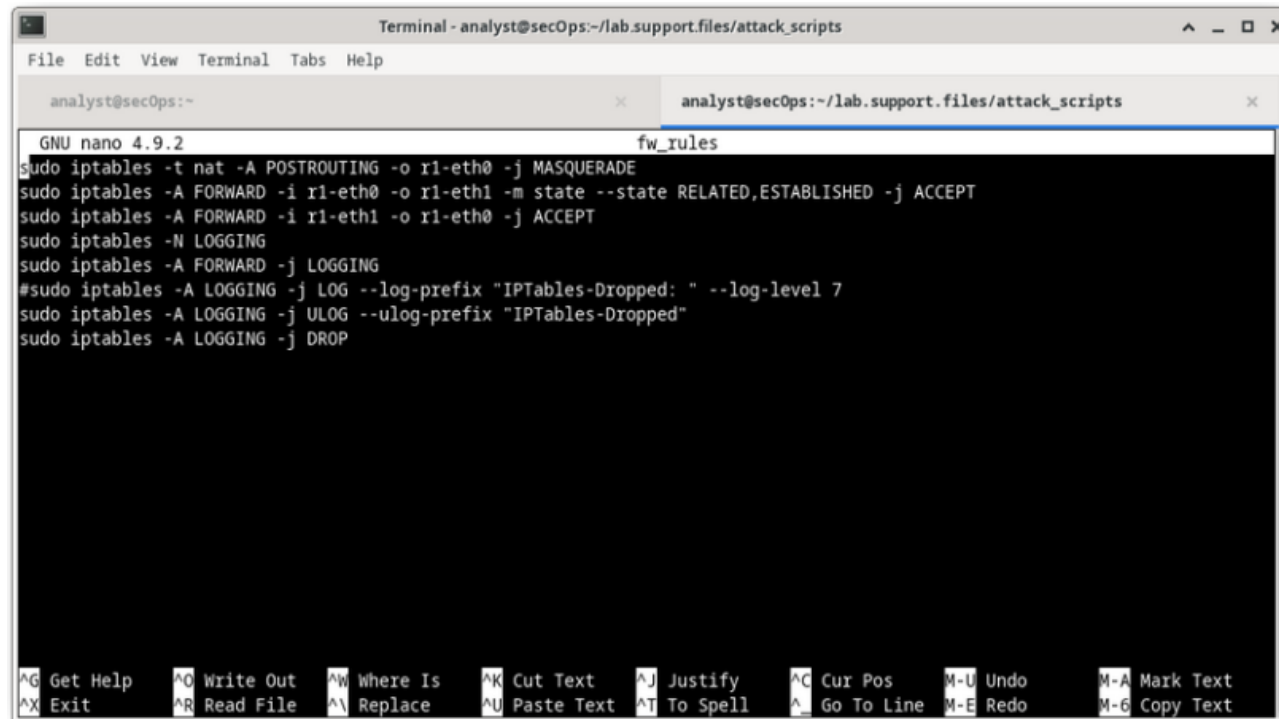
```
rod@desktop: ~  
rod@desktop:~$ uname -a  
Linux desktop 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:08 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux  
rod@desktop:~$  
rod@desktop:~$  
rod@desktop:~$ ls -l Documents/  
total 12  
drwxrwxr-x 3 rod rod 4096 Dec  8  2013 air  
drwxrwxr-x 3 rod rod 4096 Aug 13 13:24 backups  
-rw-rw-r-- 1 rod rod   0 Aug 13 13:27 configs  
-rw-rw-r-- 1 rod rod   0 Aug 13 13:27 notes  
drwxrwxr-x 2 rod rod 4096 Aug 13 13:26 OS_images  
rod@desktop:~$  
rod@desktop:~$  
rod@desktop:~$ ls -l Documents/ | grep OS  
drwxrwxr-x 2 rod rod 4096 Aug 13 13:26 OS_images  
rod@desktop:~$  
rod@desktop:~$  
rod@desktop:~$
```

# Basic Commands

Command	Description
<b>mv</b>	Moves or renames files and directories.
<b>chmod</b>	Modifies file permissions.
<b>chown</b>	Changes the ownership of a file.
<b>pwd</b>	Displays the name of the current directory.
<b>ps</b>	Lists the processes that are currently running in the system.
<b>su</b>	Simulates a login as another user or to become a superuser.
<b>sudo</b>	Runs a command as a super user, by default, or another named user.
<b>grep</b>	Used to search for specific strings of characters within a file or other command outputs.
<b>ifconfig</b>	Used to display or configure network card related information.
<b>apt-get</b>	Used to install, configure and remove packages on Debian and its derivatives.
<b>iwconfig</b>	Used to display or configure wireless network card related information.
<b>shutdown</b>	Shuts down the system and performs shut down related
<b>passwd</b>	Used to change the password.
<b>cat</b>	Used to list the contents of a file and expects the file name as the parameter.
<b>man</b>	Used to display the documentation for a specific command.

# Working with Text Files

- There are many text editors available in Linux.
- Some text editors are for the CLI only, like vi, vim, and nano.
- Other text editors, like gedit, are GUI-based.
- CLI text editors allow system management remotely, such as via SSH.



The screenshot shows a terminal window titled "Terminal - analyst@secOps:~/lab.support.files/attack\_scripts". Inside the terminal, the nano text editor is open, editing a file named "fw\_rules". The editor's title bar shows "GNU nano 4.9.2" and "fw\_rules". The file content consists of several iptables commands for setting up NAT and logging. The bottom of the terminal displays a row of keyboard shortcuts for nano, such as ^G Get Help, ^O Write Out, ^W Where Is, etc.

```
analyst@secOps:~/lab.support.files/attack_scripts$ nano fw_rules
GNU nano 4.9.2 fw_rules
sudo iptables -t nat -A POSTROUTING -o r1-eth0 -j MASQUERADE
sudo iptables -A FORWARD -i r1-eth0 -o r1-eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT
sudo iptables -A FORWARD -i r1-eth1 -o r1-eth0 -j ACCEPT
sudo iptables -N LOGGING
sudo iptables -A FORWARD -j LOGGING
#sudo iptables -A LOGGING -j LOG --log-prefix "IPTables-Dropped: " --log-level 7
sudo iptables -A LOGGING -j ULOG --ulog-prefix "IPTables-Dropped"
sudo iptables -A LOGGING -j DROP
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify    ^C Cur Pos   M-U Undo     M-A Mark Text
^X Exit      ^R Read File  ^\ Replace   ^U Paste Text ^T To Spell  ^_ Go To Line M-E Redo     M-6 Copy Text
```

# The Importance of Text Files in Linux

- In Linux, everything is treated as a file, this includes the memory, the disks, the monitor, the files, and the directories.
- The operating system as well as most programs are configured by editing the configuration files which are text files.
- Editing system or application configuration files requires super user (root) privileges. This can be accomplished with the **sudo** command.



```
GNU nano 2.7.4      File: /etc/hosts
127.0.0.1    localhost
127.0.1.1    kali

# The following lines are desirable for IPv6 capable hosts
::1         localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters

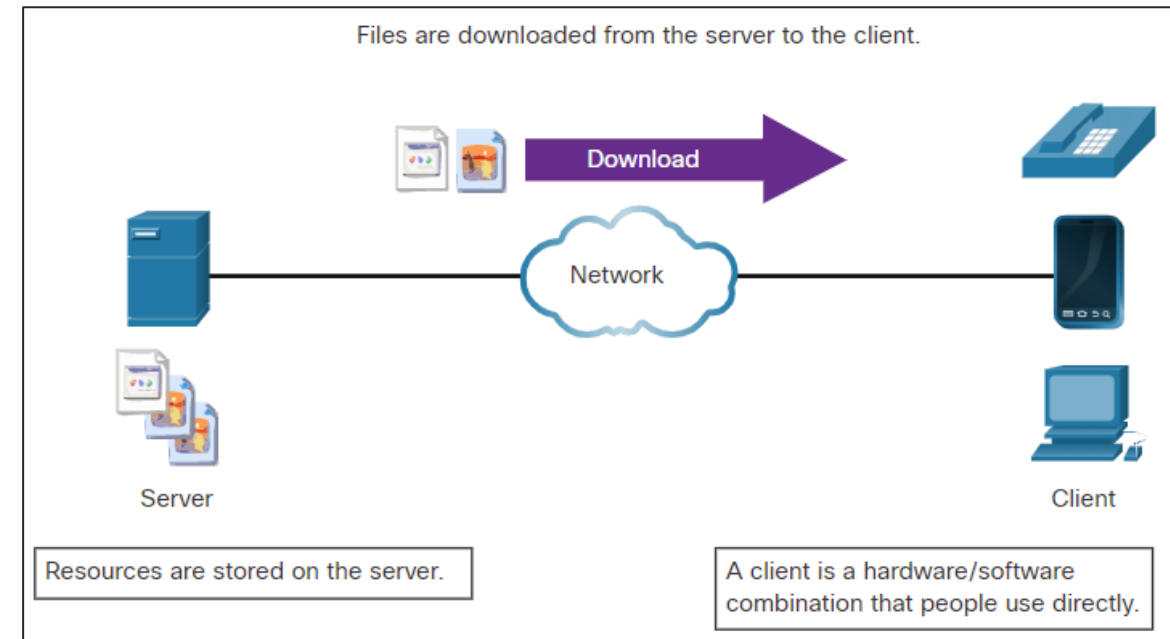
[ Read 7 lines ]
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line
```

# Linux Servers and Clients



# An Introduction to Client-Server Communications

- Servers are computers with software installed that enables them to provide services to clients across the network.
- Some provide external resources such as files, email messages, or web pages to clients upon request.
- Other services run maintenance tasks such as log management, disk scanning and so on.
- Each service requires separate server software.
- The server in the figure uses file server software to provide clients with the ability to retrieve and submit files.



# Servers, Services, and their Ports

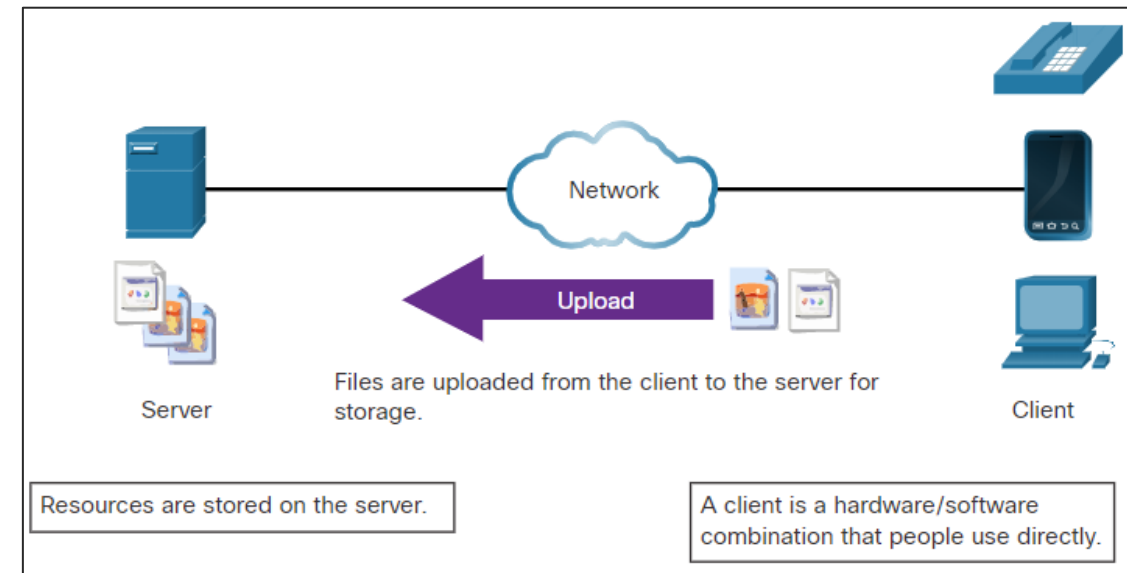
- A port is a reserved network resource used by a service.
- While the administrator can decide which port to use with any given service, many clients are configured to use a specific port by default.

Default Port Number	Service
21	File Transfer Protocol (FTP)
22	Secure Shell (SSH)
23	Telnet remote login service
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
80	Hypertext Transfer Protocol (HTTP)
110	Post Office Protocol version 3 (POP3)
123	Network Time Protocol (NTP)
143	Internet Message Access Protocol (IMAP)
161/162	Simple Network Management Protocol (SNMP)
443	HTTP Secure (HTTPS)



# Clients

- Clients are programs or applications designed to communicate with a specific type of server.
- Clients use a well-defined protocol to communicate with the server.
- Web browsers are web clients that are used to communicate with web servers through the Hyper Text Transfer Protocol on port 80.
- The File Transfer Protocol client is software used to communicate with an FTP server.
- The figure shows a client uploading files to a server.



# Basic Server Administration



# Service Configuration Files

- In Linux, services are managed using configuration files.
- Common options in configuration files are port number, location of the hosted resources, and client authorization details.
- When the service starts, it looks for its configuration files, loads them into memory, and adjusts itself according to the settings in the files.
- The command output shows a portion of the configuration file for Nginx, which is a lightweight web server for Linux.

```
[analyst@secOps ~]$ cat /etc/nginx/nginx.conf
#user html;
worker_processes 1;
#error_log logs/error.log;
#error_log logs/error.log notice;
#error_log logs/error.log info;
#pid logs/nginx.pid;
events {
    worker_connections 1024;
}
http {
    include mime.types;
    default_type application/octet-stream;
    #log_format main '$remote_addr - $remote_user [$time_local] "$request" '
    #                '$status $body_bytes_sent "$http_referer" '
    #                '"$http_user_agent" "$http_x_forwarded_for"';
    #access_log logs/access.log main;
```

# Hardening Devices

- Device hardening involves implementing proven methods of securing the device and protecting its administrative access.
- The following are basic best practices for device hardening:
  - Ensure physical security
  - Minimize installed packages
  - Disable unused services
  - Use SSH and disable the root account login over SSH
  - Keep the system updated
  - Disable USB auto-detection
  - Enforce strong passwords
  - Force periodic password changes
  - Keep users from re-using old passwords

# Monitoring Service Logs

- Log files are the records that a computer stores to keep track of important events. Kernel, services, and application events are all recorded in log files.
- By monitoring Linux log files, an administrator gains a clear picture of the computer's performance, security status, and any underlying issues.
- In Linux, log files can be categorized as:

- Application logs
- Event logs
- Service logs
- System logs

Log	Purpose
/var/log/messages	Used to store informational and non-critical system messages
/var/log/auth.log	Stores all authentication-related events
/var/log/secure	Used by RedHat and CentOS and tracks sudo logins, SSH logins, and errors logged by SSSD
/var/log/boot.log	Stores boot related messages during startup
/var/log/dmesg	Contains kernel ring bugger messages
/var/log/kern.log	Contains information logged by the kernel
/var/log/cron	A service used for scheduling automated tasks in Linux
/var/log/mysqld.log or /var/log/mysql.log	Logs all debug, failure and success messages related to the mysql process and mysqld_safe daemon

# The Linux File System



# The File System Types in Linux

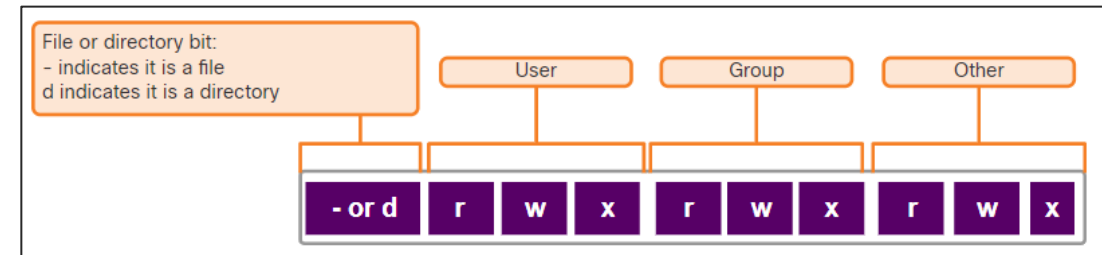
File System Type	Description
ext2 (second extended file system)	Is the file system of choice for flash-based storage media.
ext3 (third extended file system)	Is an improved successor to ext2 with the additional feature of journaling of all the file system changes.
ext4 (fourth extended file system)	Is designed as a successor to ex3 with increased support file sizes and better performance than ext3.
NFS (Network File System)	Is a network-based file system, allowing file access over the network.
CDFS (Compact Disc File System)	Was created specifically for optical disk media.
Swap File System	Is used when the system runs out of RAM.
HFS+ (Hierarchical File System Plus)	Is the primary file system used by Apple in its Macintosh computers.
APFS (Apple File System)	An updated file system used by Apple devices that provides strong encryption and is optimized for flash and solid-state drives.
Master Boot Record (MBR)	Is located in the first sector of a partitioned computer and stores all the information about the way the file system is organized.



# Linux Roles and File Permissions

- Linux uses file permissions in order to organize the system and enforce boundaries within the computer.
- Octal values are used to define permissions.

Binary	Octal	Permission	Description
000	0	---	No access
001	1	--x	Execute only
010	2	-w-	Write only
011	3	-wx	Write and Execute
100	4	r--	Read only
101	5	r-x	Read and Execute
110	6	rw-	Read and Write
111	7	rwX	Read, Write and Execute



# Hard Links and Symbolic Links

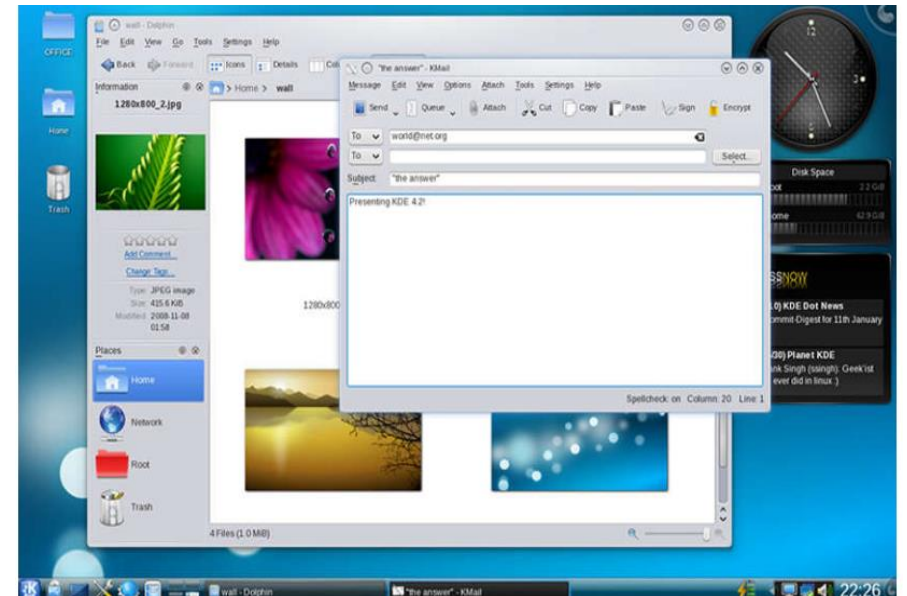
- The *ln* command make links between files.
- Hard Links:
  - Points to the same location as the original file.
  - Changes one file, the other one also changes.
- Symbolic or Soft Links:
  - Uses the *-s* option in the command to create the symbolic link.
  - Delete the original file, the soft link is link to the original file that no longer exists.
- Advantages to symbolic link:
  - Locating hard links is more difficult.
  - Hard links are limited to the file system in which they are created. Symbolic links can link to a file in another file system.
  - Hard links cannot link to a directory, but symbolic links can.

# Working on a Linux Host



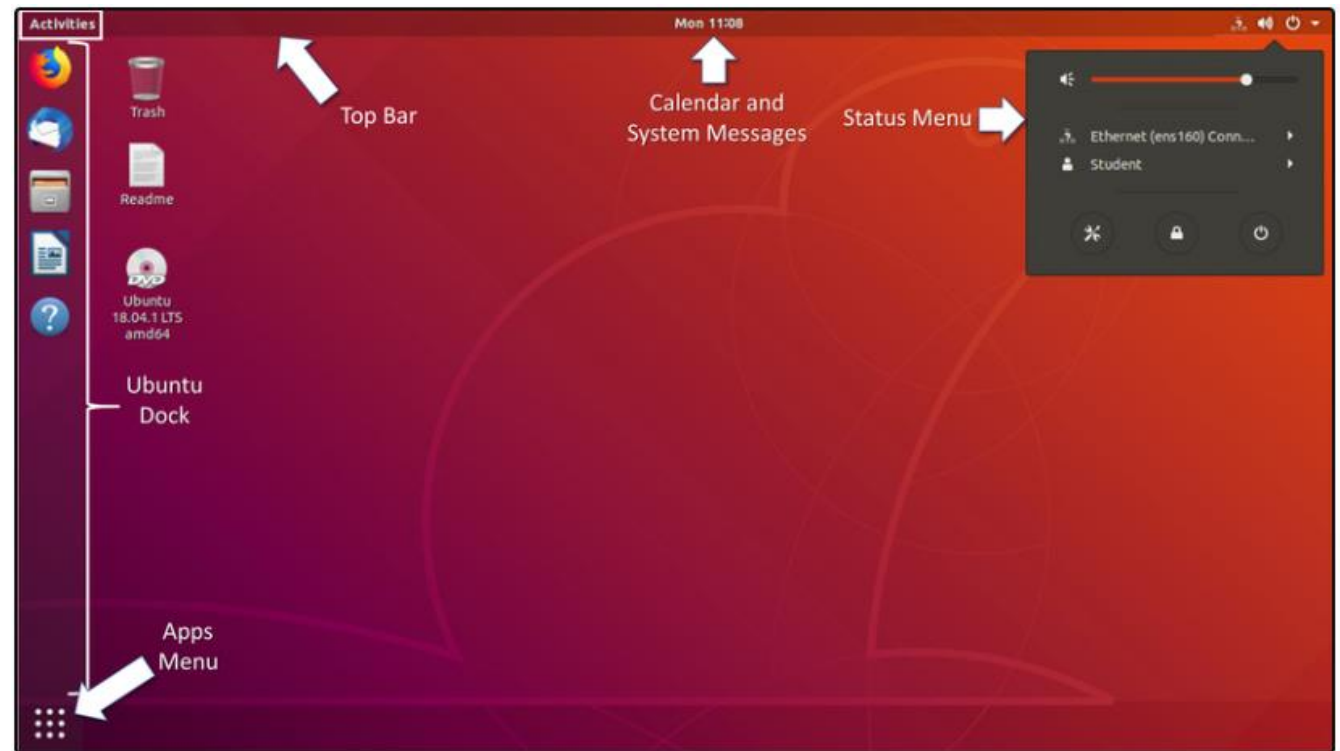
# X Windows System

- X Window System is the framework for the Linux GUI also known as X and X11.
- Functions for drawing and moving the window, as well as interacting with the mouse and keyboard.
- X works as a server and can send the graphical window over a network to a remote computer.
- X does not specify the user interface or desktop. That is left to a window manager to define the look and feel of the GUI.
- Gnome and KDE are examples of popular Linux window managers.



# The Linux GUI

- While an operating system does not require a GUI to function, GUIs are considered more user-friendly than the CLI. The Linux GUI as a whole can be easily replaced by the user.
- Ubuntu is a very popular and user-friendly Linux distribution.
- Ubuntu Linux uses Gnome 3 as its default GUI.
- The figure shows the location of some of the features of the Ubuntu Gnome 3 Desktop.



# Installing and Running Applications on a Linux Host

- Many end-user applications are complex programs written in compiled languages.
- To aid in the installation process, Linux includes programs called package managers.
- By using a package manager to install a package, all the necessary files are placed in the correct file system location.
- A package is the term used to refer to a program and all its supporting files.
- The command output shows the output of a few apt-get commands used in Debian distributions.

```
analyst@cuckoo:~$ sudo apt-get update
[sudo] password for analyst:
Hit:1 http://us.archive.ubuntu.com/ubuntu xenial InRelease
Get:2 http://us.archive.ubuntu.com/ubuntu xenial-updates InRelease [102 kB]
Get:3 http://security.ubuntu.com/ubuntu xenial-security InRelease [102 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu xenial-backports InRelease [102 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64 Packages [534 kB]
<output omitted>
Fetched 4,613 kB in 4s (1,003 kB/s)
Reading package lists... Done
analyst@cuckoo:~$
analyst@cuckoo:~$ sudo apt-get upgrade
Reading package lists Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages have been kept back:
linux-generic-hwe-16.04 linux-headers-generic-hwe-16.04
linux-image-generic-hwe-16.04
The following packages will be upgraded:
firefox firefox-locale-en gir1.2-javascriptcoregtk-4.0 gir1.2-webkit2-4.0 libjavascriptcoregtk-4.0-18
libwebkit2gtk-4.0-37 libwebkit2gtk-4.0-37-gtk2 libxext4 libxext4-dev linux-libc-dev logrotate
openssh-client
qemu-block-extra qerau-kvm qemu-system-common qemu-system-x86 qemu-utils
```

# Keeping the System Up to Date

- OS updates, also known as patches, are released periodically by OS companies to address any known vulnerabilities in their operating systems.
- Modern operating systems will alert the user when updates are available for download and installation, but the user can check for updates at any time.
- The following table compares Arch Linux and Debian/Ubuntu Linux distribution commands to perform package system basic operations.

Task	Arch	Debian/Ubuntu
Install a package by name	<b>pacman -S</b>	<b>apt install</b>
Remove a package by name	<b>pacman -Rs</b>	<b>apt remove</b>
Update a local package	<b>pacman -Syy</b>	<b>apt-get update</b>
Upgrade all currently installed packages	<b>pacman -Syu</b>	<b>apt-get upgrade</b>



# Processes and Forks

- A process is a running instance of a computer program. Multitasking operating systems can execute many processes at the same time.
- Forking is a method that the kernel uses to allow a process to create a copy of itself to provide process scalability.
- Some commands to manage processes:

Command	Description
<b>ps</b>	<ul style="list-style-type: none"><li>• Used to list the processes running on the computer at the time it is invoked.</li><li>• It can be instructed to display running processes that belong to the current user or other users.</li></ul>
<b>top</b>	<ul style="list-style-type: none"><li>• Used to list running processes, but unlike <b>ps</b>, <b>top</b> keeps displaying running processes dynamically.</li><li>• Press <b>q</b> to exit top.</li></ul>
<b>kill</b>	<ul style="list-style-type: none"><li>• Used to modify the behavior of a specific process.</li><li>• Depending on the parameters, <b>kill</b> will remove, restart, or pause a process.</li><li>• In many cases, the user will run <b>ps</b> or <b>top</b> before running kill.</li><li>• This is done so the user can learn the PID of a process before running kill.</li></ul>

# Malware on a Linux Host

- Linux malware includes viruses, Trojan horses, worms, and other types of malware that can affect the operating system.
- A common Linux attack vector is its services and processes.
- The command output shows an attacker using the Telnet command to probe the nature and version of a web server (port 80).
- The attacker has learned that the server is running nginx version 1.12.0. The next step would be to research known vulnerabilities in the nginx 1.12.0 code.

```
analyst@secOps ~]$ telnet 209.165.200.224 80
Trying 209.165.200.224...
Connected to 209.165.200.224.
Escape character is '^]'.
<type anything to force an HTTP error response>
HTTP/1.1 400 Bad Request
Server: nginx/1.12.0
Date: Wed, 17 May 2017 14:27:30 GMT
Content-Type: text/html
Content-Length: 173
Connection: close
<html>
<head><title>400 Bad Request</title></head>
<body bgcolor="white">
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx/1.12.0</center>
</body>
</html >
Connection closed by foreign host.
analyst@secOps ~]$
```

# Rootkit Check

- A rootkit is a type of malware designed to increase an unauthorized user's privileges or grant access to portions of the software that should not normally be allowed.
- Rootkit detection methods include booting the computer from a trusted media.
- Rootkit removal can be complicated. Re-installation of the operating system is the only real solution to the problem.
- **chkrootkit** is a popular Linux-based program designed to check the computer for known rootkits.
- The command output shows the output of **chkrootkit** on an Ubuntu Linux.

```
analyst@cuckoo:~$ sudo ./chkrootkit
[sudo] password for analyst:
ROOTDIR is '/'
Checking 'amd'... not found
Checking 'basename'... not infected
Checking 'biff'... not found
Checking 'chfn'... not infected
Checking 'chsh'... not infected
Checking 'cron'... not infected
Checking 'crontab'... not infected
Checking 'date'... not infected
Checking 'du'... not infected
Checking 'dirname'... not infected
Checking 'echo'... not infected
Checking 'egrep'... not infected
Checking 'env'— not infected
Checking 'find'... not infected
Checking 'fingerd'... not found
Checking 'gpm'... not found
Checking 'grep'... not infected
Checking 'hdparm'... not infected
Checking 'su'... not infected
Checking 'ifconfig'... not infected
Checking 'inetd'... not tested
Checking 'inetdconf'... not found
```

# Piping Commands

- Many commands can be combined to perform more complex tasks by a technique known as piping.
- the pipe (|)
- Piping consists of chaining commands together, feeding the output of one command into the input of another.
- For example, the two commands, **ls** and **grep**, can be piped together to filter out the output of **ls**. This is shown in the output of the **ls -l | grep host** command and the **ls -l | grep file** command.

```
[analyst@secOps ~]$ ls -l
total 40
drwxr-xr-x 2 analyst analyst 4096 Mar 22 2018 Desktop
drwxr-xr-x 3 analyst analyst 4096 April 2 14:44 Downloads
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile1.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile2.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:52 hostfile3.txt
drwxr-xr-x 9 analyst analyst 4096 Jul 19 2018 lab.support.files
-rw-r--r-- 1 analyst analyst 19 May 20 10:53 mytest.com
-rw-r--r-- 1 analyst analyst 228844 May 20 10:54 rkhunter-1.4.6-1-any.pkg.tar.xz
drwxr-xr-x 2 analyst analyst 4096 Mar 21 2018 second_drive
-rw-r--r-- 1 analyst analyst 257 May 20 10:52 space.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ ls -l | grep host
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile1.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile2.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:52 hostfile3.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ ls -l | grep file
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile1.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile2.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:52 hostfile3.txt
drwxr-xr-x 9 analyst analyst 4096 Jul 19 2018 lab.support.files
[analyst@secOps ~]$
```



# Networking **CISCO** Academy



[ice.aiub.edu](http://ice.aiub.edu)



[ice@aiub.edu](mailto:ice@aiub.edu)



01630-665666