

Module 3: The Windows Operating System

Instructor Materials

CyberOps Associate v1.0

Module 3: The Windows Operating System

Module Objectives

- Module Title: The Windows Operating System
- Module Objective: Explain the security features of the Windows operating system.

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

3.1 Windows History

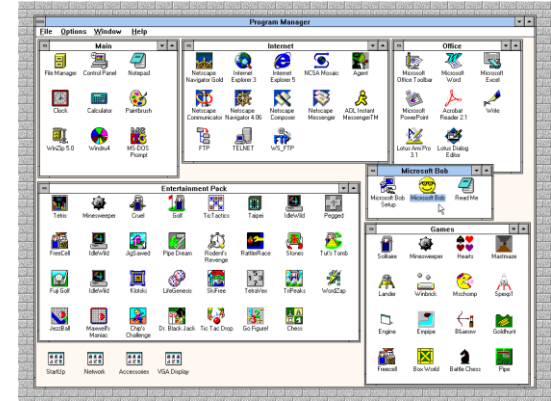
Disk Operating System

- The Disk Operating System (DOS) is an operating system that the computer uses to enable the data storage devices to read and write files.
- DOS provides a file system which organizes the files in a specific way on the disk.
- MS-DOS, created by Microsoft, used a command line as the interface for people to create programs and manipulate data files. DOS commands are shown in bold text in the given command output.
- With MS-DOS, the computer had a basic working knowledge of accessing the disk drive and loading the operating system files directly from disk as part of the boot process.

```
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:\>
```

Disk Operating System (Contd.)

- Early versions of Windows consisted of a Graphical User Interface (GUI) that ran over MS-DOS, starting with Windows 1.0 in 1985.
- In newer versions of Windows, built on New Technologies (NT), the operating system itself is in direct control of the computer and its hardware.
- Today, many things that used to be accomplished through the command line interface of MS-DOS can be accomplished in the Windows GUI.
- To experience a little of MS-DOS, open a command window by typing cmd in Windows Search and pressing Enter.



Disk Operating System (Contd.)

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

MS-DOS Command	Description
dir	Shows a listing of all the files in the current directory (folder)
cd <i>directory</i>	Changes the directory to the indicated directory
cd ..	Changes the directory to the directory above the current directory
cd \	Changes the directory to the root directory (often C:)
copy <i>source destination</i>	Copies files to another location
del <i>filename</i>	Deletes one or more files
find	Searches for text in files
mkdir <i>directory</i>	Creates a new directory
ren <i>oldname newname</i>	Renames a file
help	Displays all the commands that can be used, with a brief description
help <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** (OS).
 - Protection of memory
 - Preemptive multitasking
- Many editions were built specifically for workstation, professional, server, advanced server, and datacenter server, to name just a few of the many purpose-built versions.
- The 64-bit operating system was an entirely new architecture. It had a 64-bit address space instead of a 32-bit address space.
- 64-bit computers and operating systems are backward-compatible with older, 32-bit programs, but 64-bit programs cannot be run on older, 32-bit hardware.

Windows Versions (Contd.)

The following table lists common Windows versions:

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

Operating System Vulnerabilities

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

Operating System Vulnerabilities (Contd.)

The following table lists some common Windows OS Security recommendations:

Recommendation	Description
Virus or malware protection	<ul style="list-style-type: none">• By default, Windows uses Windows Defender for malware protection.• Windows Defender provides a suite of protection tools built into the system.• If Windows Defender is turned off, the system becomes more vulnerable to attacks and malware.
Unknown or unmanaged services	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• A good security policy must be configured and followed.• Many settings in the Windows Security Policy control can prevent attacks.

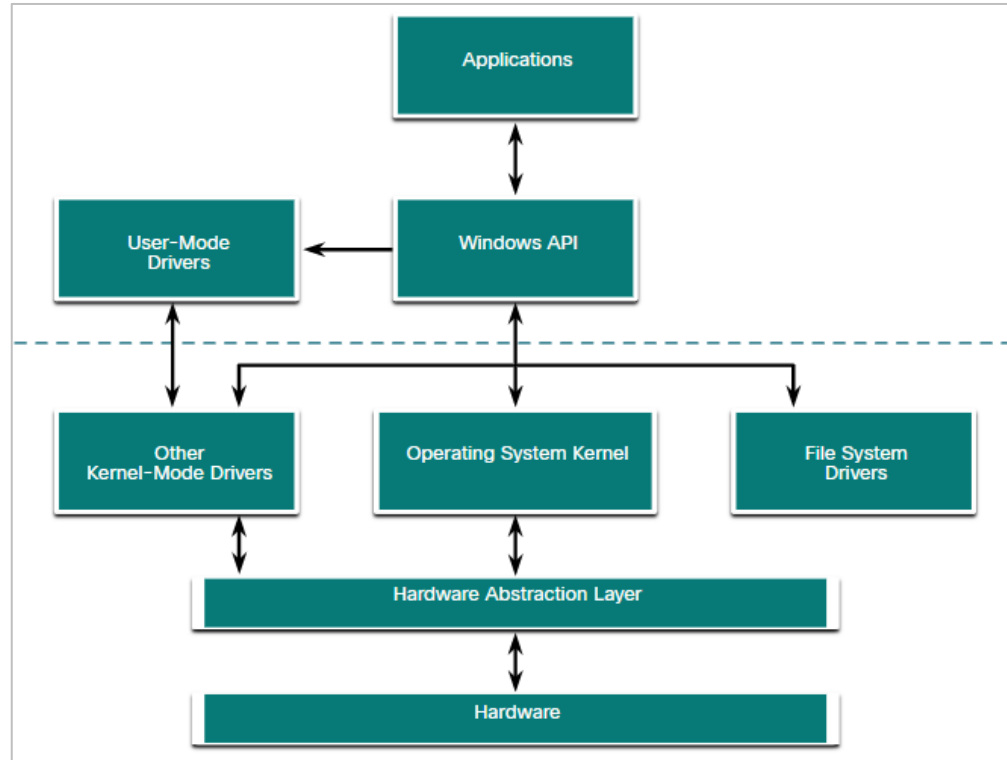
Operating System Vulnerabilities (Contd.)

Recommendation	Description
Firewall	<ul style="list-style-type: none">• By default, Windows uses Windows Firewall to limit communication with devices on the network. Over time, rules may no longer apply.• 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	<ul style="list-style-type: none">• These permissions must be set correctly. It is easy to give the “Everyone” group Full Control, but this allows all people to access 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• When a user logs in as an administrator, any program that they run will have the privileges of that account.• It is best to log in as a Standard User and only use the administrator password to accomplish certain tasks.

3.2 Windows Architecture and Operations

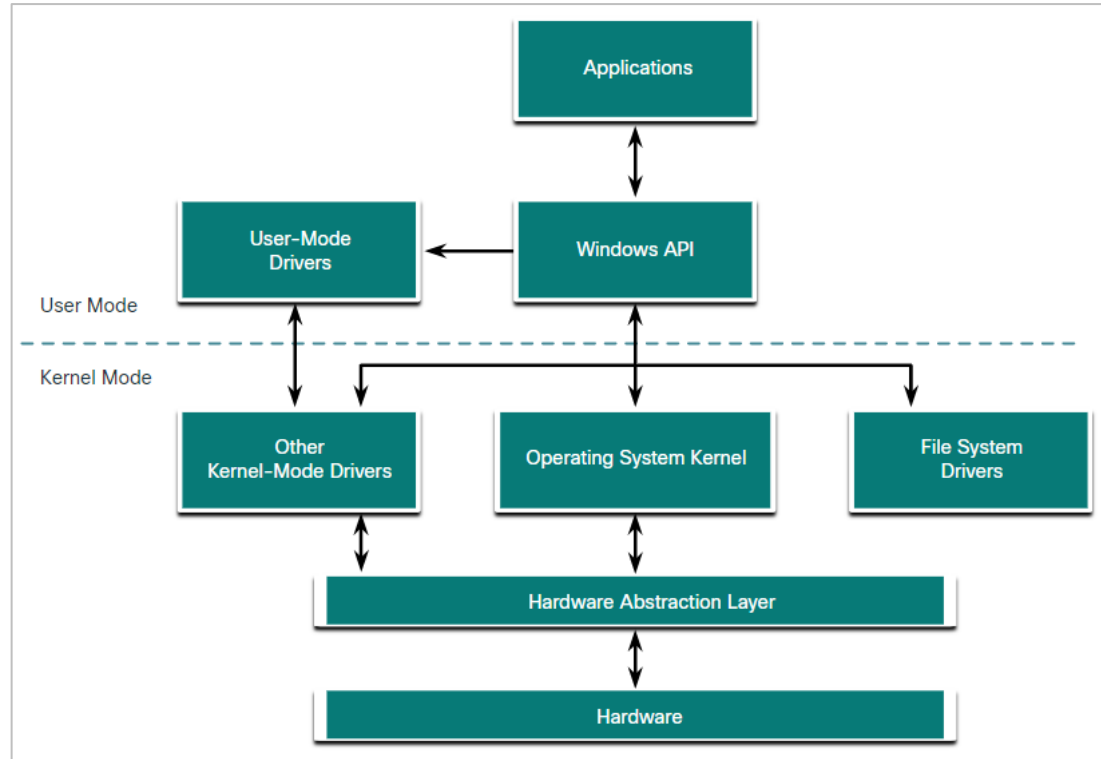
Hardware Abstraction Layer

- 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.
- The basic Windows architecture is shown in the figure.



User Mode and Kernel Mode

- The two different modes in which a CPU operates when the computer has Windows installed are 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

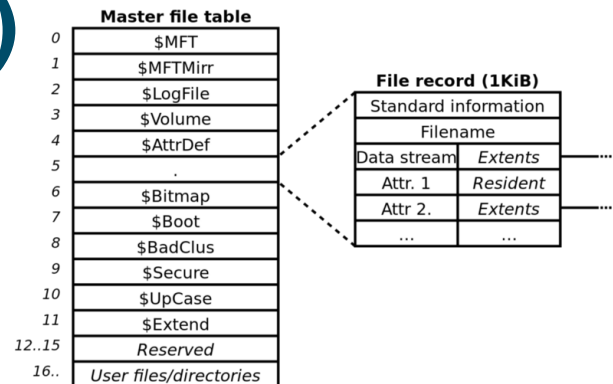
Windows File System	Description
exFAT	<ul style="list-style-type: none">• This is a simple file system supported by many different operating systems.• FAT has limitations to the number of partitions, partition sizes, and file sizes that it can address, so it is not usually used for hard drives or solid-state drives anymore.• Both FAT16 and FAT32 are available to use, with FAT32 being the most common as it has many fewer restrictions than FAT16.
Hierarchical File System Plus (HFS+)	<ul style="list-style-type: none">• This file system is used on MAC OS X computers and allows much longer filenames, file sizes, and partition sizes.• Although it is not supported by Windows without special software, Windows is able to read data from HFS+ partitions.

Windows File Systems (Contd.)

Windows File System	Description
Extended File System (EXT)	<ul style="list-style-type: none">• 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)	<ul style="list-style-type: none">• This is the most commonly used file system when installing Windows. All versions of Windows and Linux support NTFS.• Mac-OS X computers can only read an NTFS partition. They are able to write to an NTFS partition after installing special drivers.

Windows File Systems (Contd.)

- NTFS formatting creates important structures on the disk for file storage, and tables for recording the locations of files:
 - Partition Boot Sector: This is the first 16 sectors of the drive. It contains the location of the Master File Table (MFT). The last 16 sectors contain a copy of the boot sector.
 - Master File Table (MFT): This table contains the locations of all the files and directories on the partition, including file attributes such as security information and timestamps.
 - System Files: These are hidden files that store information about other volumes and file attributes.
 - File Area: The main area of the partition where files and directories are stored.
- **Note:** *When formatting a partition, the previous data may still be recoverable because not all the data is completely removed. 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.*



```
Administ x Administ x + v - □ x
NtfsInfo v1.2 - NTFS Information Dump
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Volume Size
-----
Volume size       : 1023881 MB
Total sectors     : 2096910335
Total clusters    : 262113791
Free clusters     : 124107540
Free space        : 484795 MB (47% of drive)

Allocation Size
-----
Bytes per sector  : 512
Bytes per cluster : 4096
Bytes per MFT record : 0
Clusters per MFT record: 0

MFT Information
-----
MFT size          : 285 MB (0% of drive)
MFT start cluster : 786432
MFT zone clusters : 21555584 - 21585920
MFT zone size     : 118 MB (0% of drive)
MFT #mirror start : 2

Meta-Data files
```

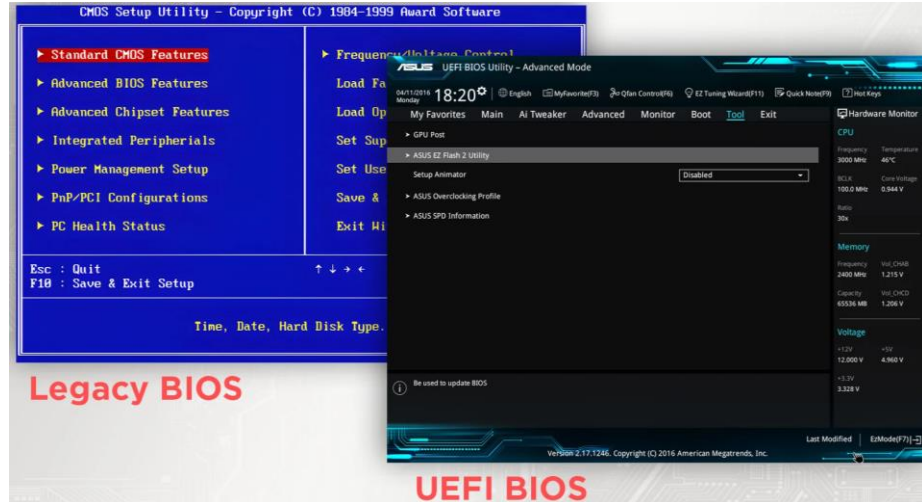
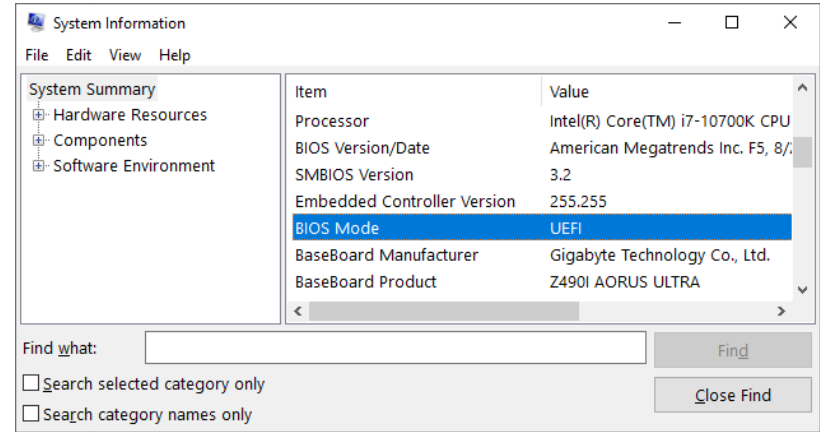
Alternate Data Streams

- 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, Alternate Data Streams (ADSs) can be connected to the file.
- 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:ADS. This filename indicates an ADS called ADS is associated with the file called Testfile.txt.

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

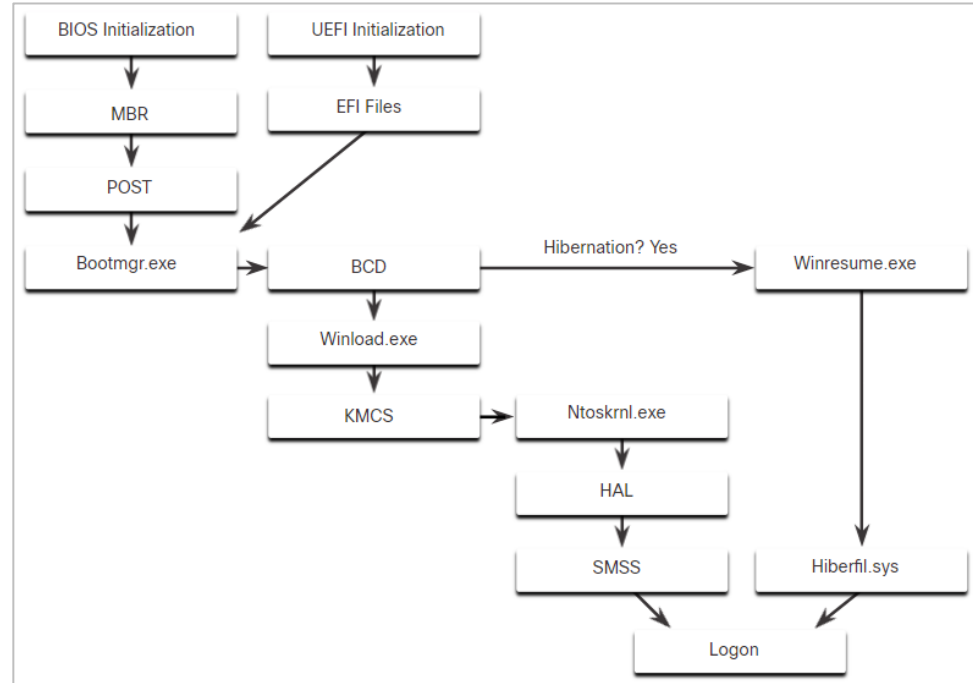
Windows Boot Process

- 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 (Contd.)

- 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.
- **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.

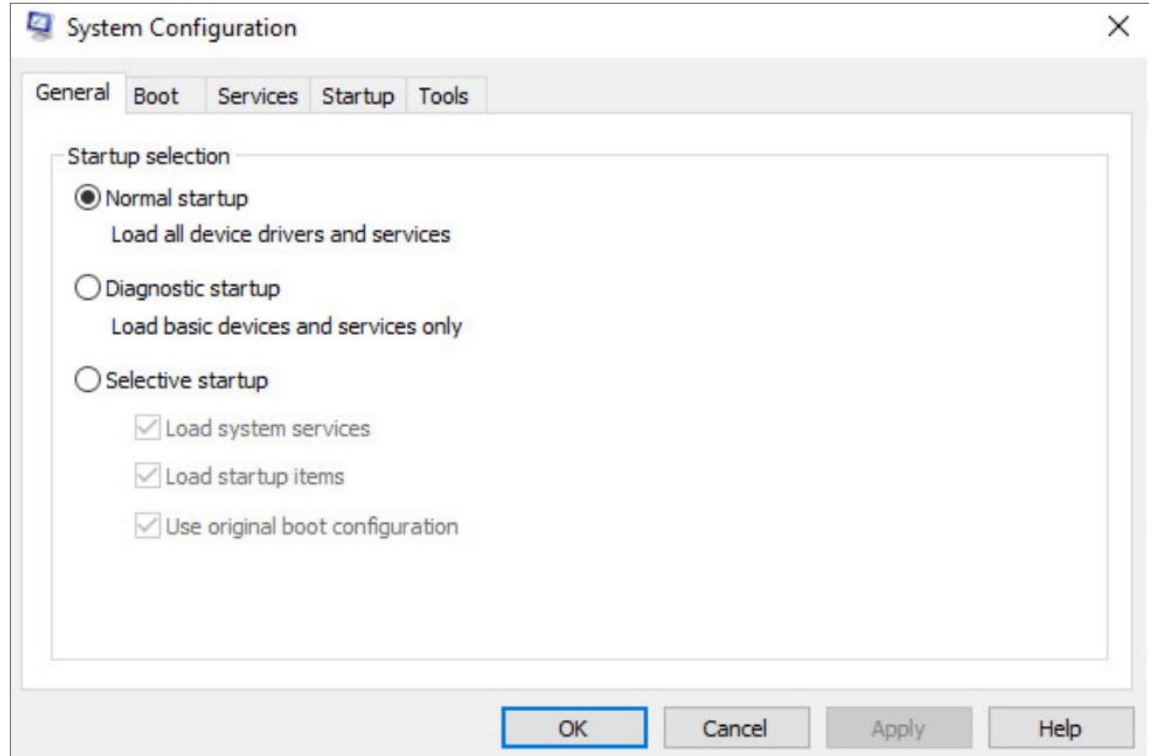


Windows Startup

- There are two important registry items that are used to automatically start applications and services:
 - `HKEY_LOCAL_MACHINE` - Several aspects of Windows configuration are stored in this key, including information about services that start with each boot.
 - `HKEY_CURRENT_USER` - Several aspects related to the logged in user are stored in this key, including information about services that start only when the user logs on to the computer.
- Different entries in these registry locations define which services and applications will start, as indicated by their entry type.
- These types include *Run*, *RunOnce*, *RunServices*, *RunServicesOnce*, and *Userinit*. These entries can be manually entered into the registry, but it is much safer to use the `Mscconfig.exe` tool.
- The `services.msc` or `Mscconfig` tool is used to view and change all of the start-up options for the computer. It opens the System Configuration window.

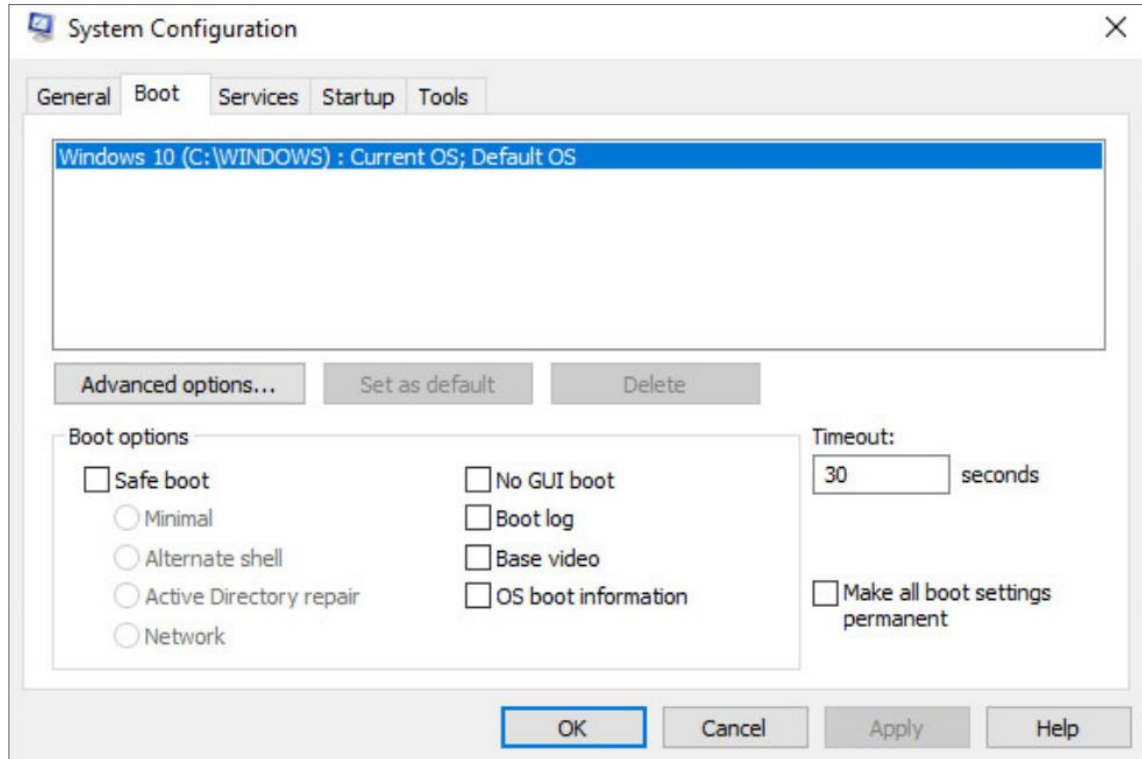
Windows Startup (Contd.)

- There are five tabs that 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.



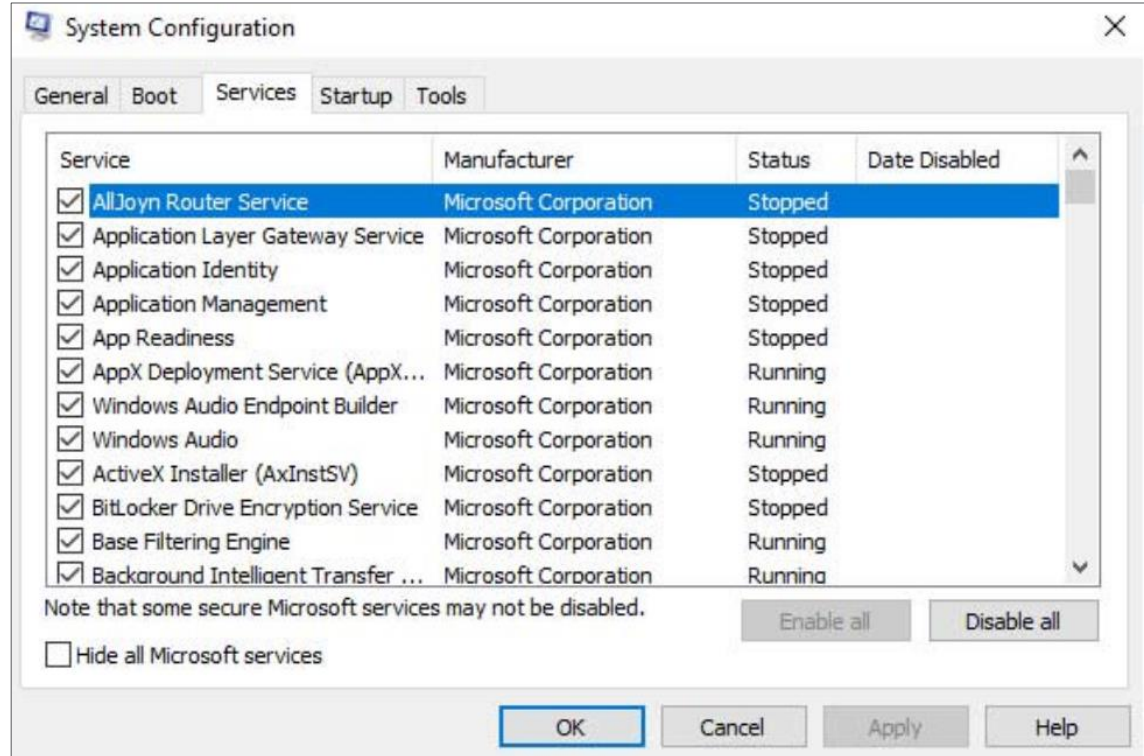
Windows Startup (Contd.)

- Boot
- Any installed operating system can be chosen here to start.
- There are also options for Safe boot, which is used to troubleshoot startup.



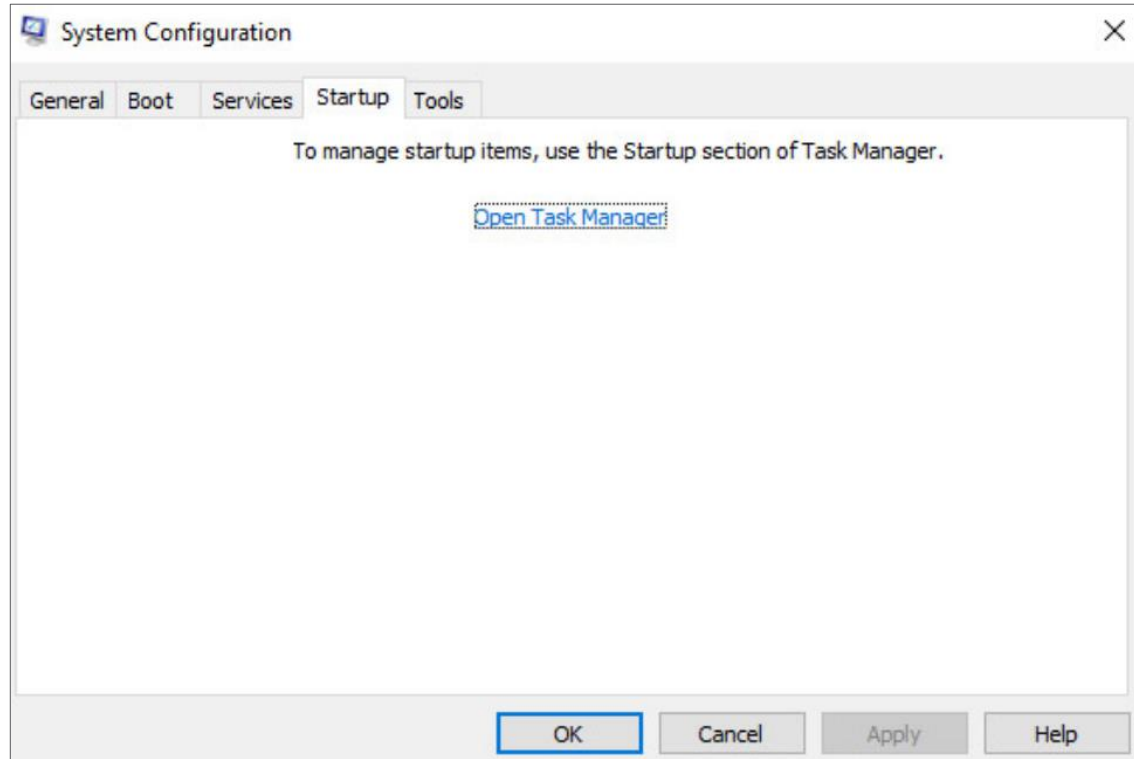
Windows Startup (Contd.)

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



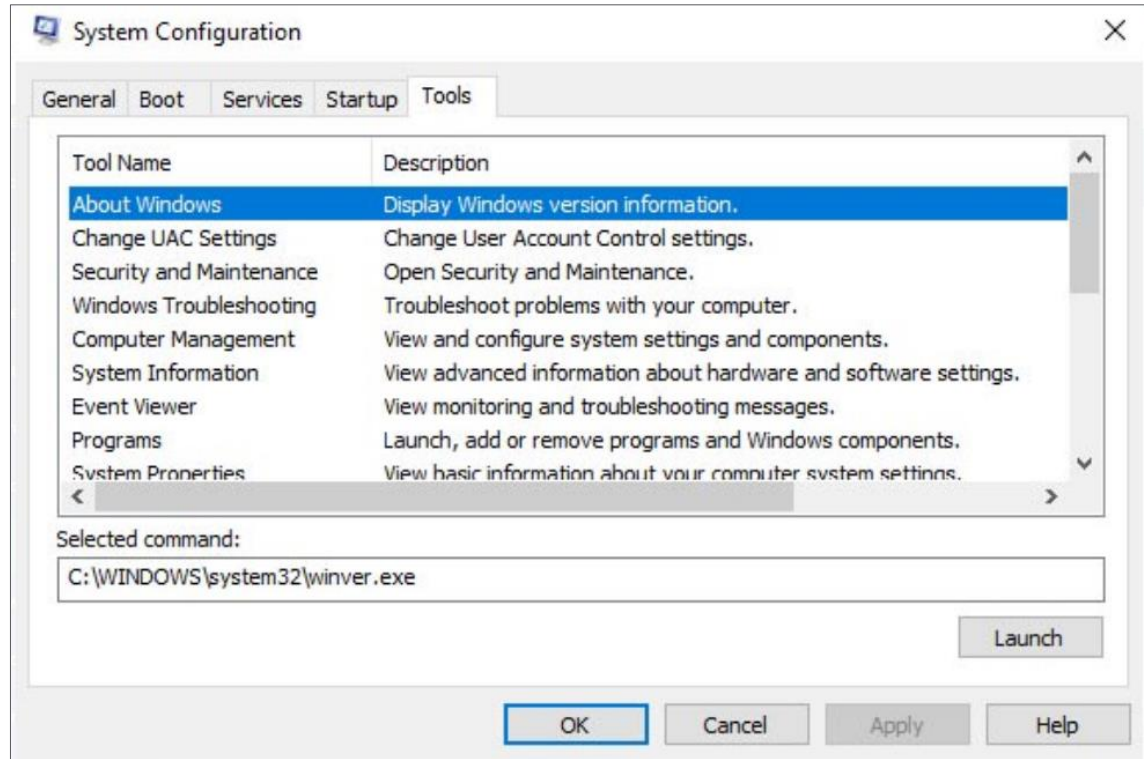
Windows Startup (Contd.)

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



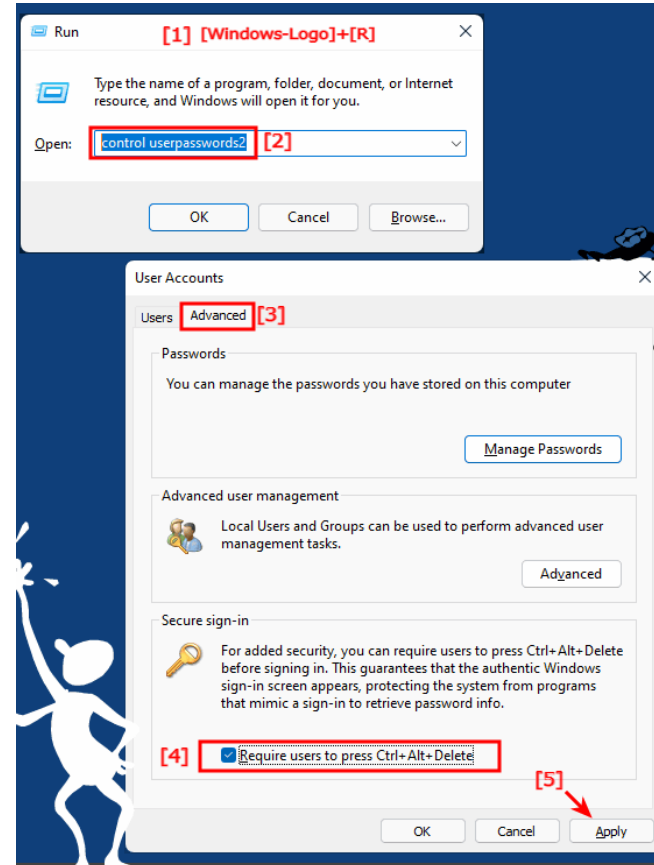
Windows Startup (Contd.)

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



Windows Shutdown

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



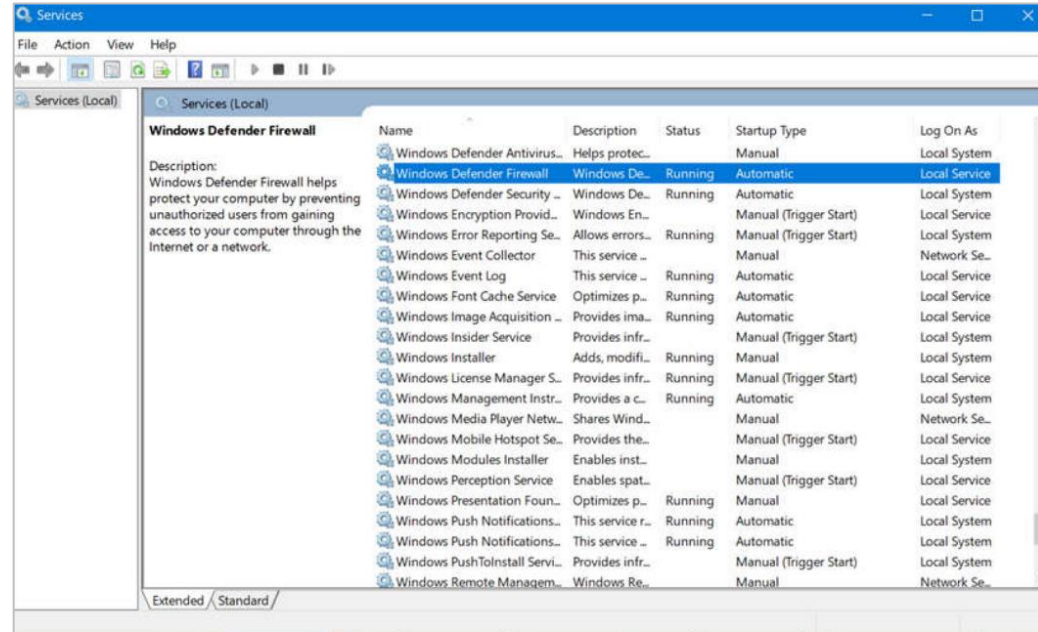
Processes, Threads, and Services

- 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.
- To configure Windows processes, search for Task Manager. The Processes tab of the Task Manager is shown in the figure.
- All of the threads dedicated to a process are contained within the same address space which means that these threads may not access the address space of any other process. This prevents corruption of other processes.

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

Processes, Threads, and Services (Contd.)

- Some of the processes that Windows runs are services. These are programs that run in the background to support the operating system and applications.
- Services provide long-running functionality, such as wireless or access to an FTP server.
- To configure Windows Services, search for services. The Windows Services control panel applet is shown in the figure.
- Be very careful when manipulating the settings of these services. Shutting down a service may adversely affect applications or other services.

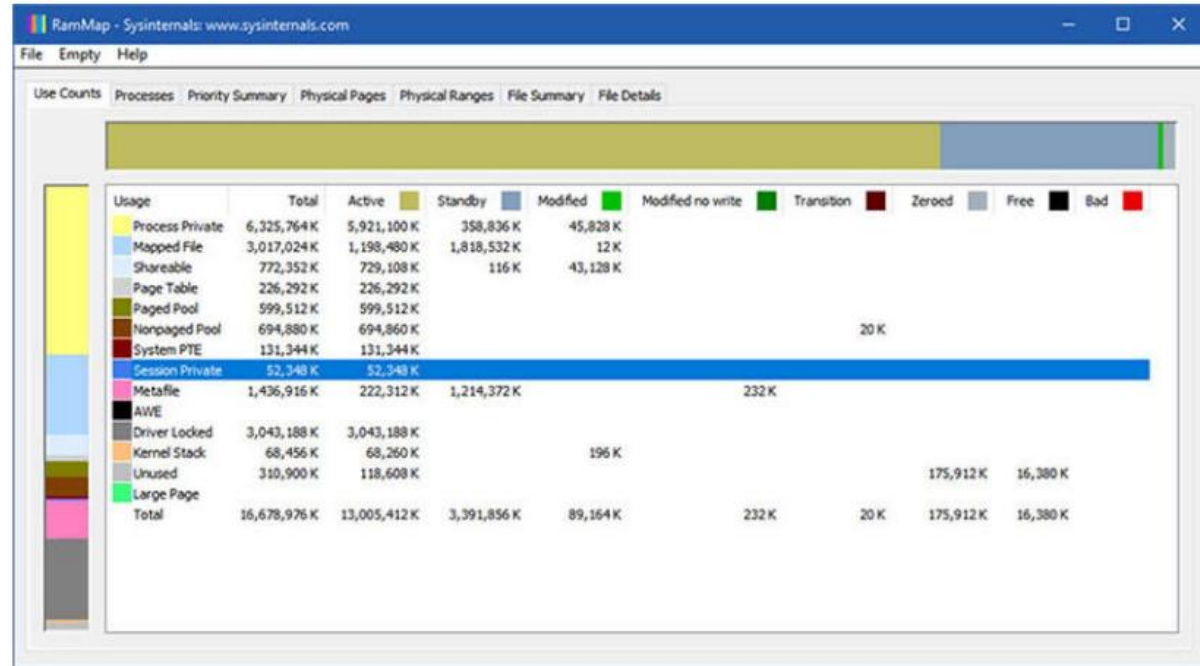


Memory Allocation and Handles

- 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.
- As 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.

Memory Allocation and Handles (Contd.)

- A powerful tool for viewing memory allocation is RAMMap, which is shown in the figure.
- RAMMap is part of the Windows Sysinternals Suite of tools. It can be downloaded from Microsoft.
- RAMMap provides information regarding how Windows has allocated system memory to the kernel, processes, drivers, and applications.



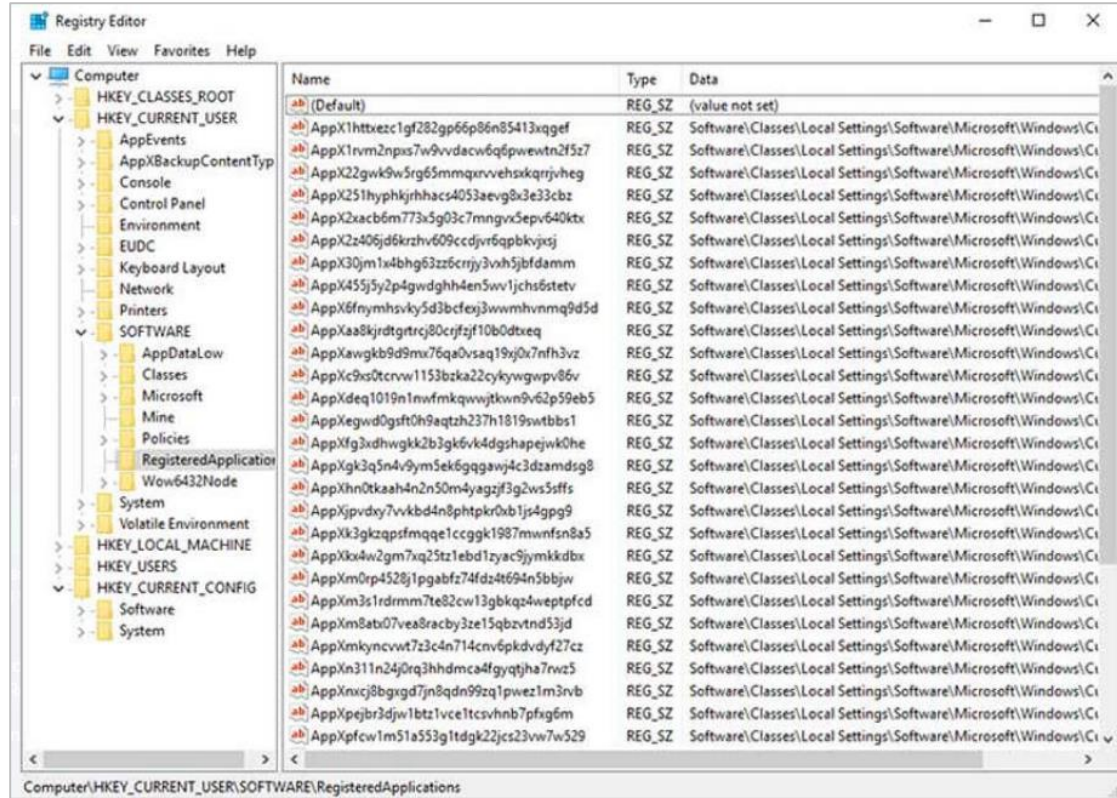
The Windows Registry

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

The Windows Registry (Contd.)

- New hives cannot be created. The registry keys and values in the hives can be created, modified, or deleted by an account with administrative privileges.
- As shown in the figure, the tool `regedit.exe` is used to modify the registry.
- Be very careful when using this tool. Minor changes to the registry can have massive or even catastrophic effects.



The Windows Registry (Contd.)

- 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.
- The path is displayed at the bottom of the window for reference.
- Registry keys can contain either a subkey or a value. The different values that keys can contain are as follows:
 - REG_BINARY: Numbers or Boolean values
 - REG_DWORD: Numbers greater than 32 bits or raw data
 - REG_SZ: String values
- 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.

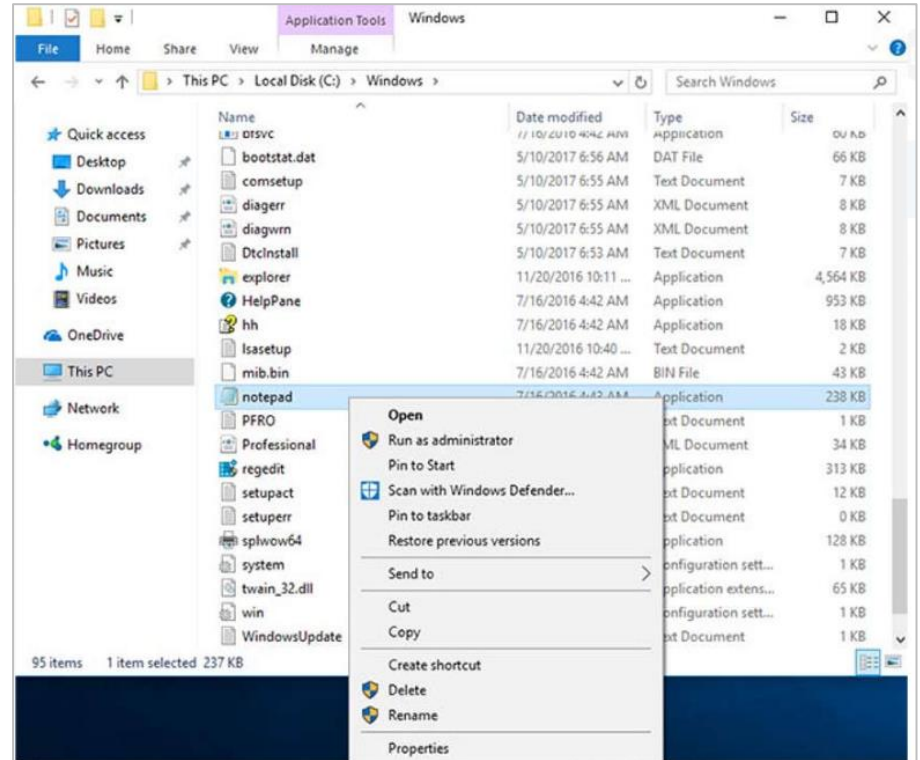
Lab - Exploring Processes, Threads, Handles, and Windows Registry

- In this lab, you will complete the following objectives:
- Explore the processes, threads, and handles using Process Explorer in Sysinternals Suite.
- Use the Windows Registry to change a setting.

3.3 Windows Configuration and Monitoring

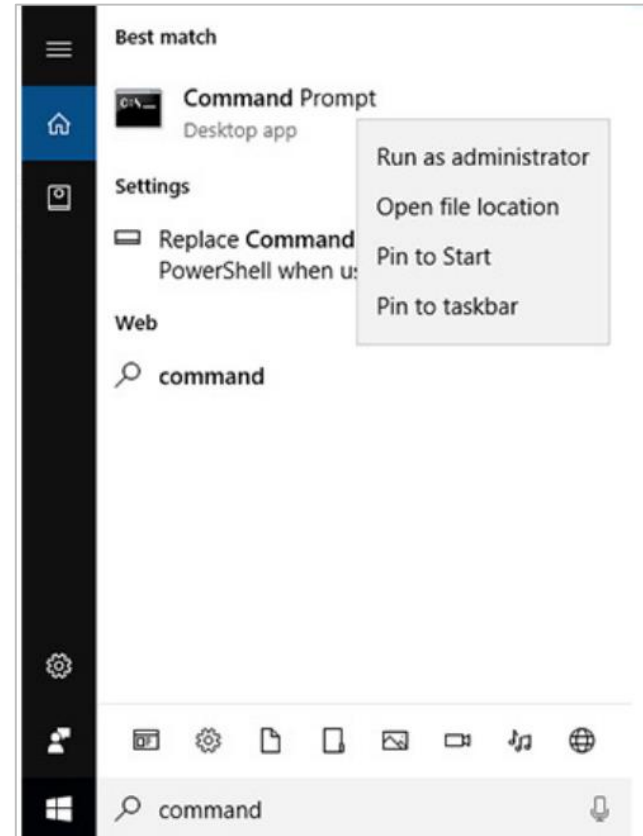
Run as Administrator

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



Run as Administrator (Contd.)

- Administrator Command Prompt
- Search for command, right-click the executable file, and choose Run as Administrator from the Context Menu.
- Every command that is executed from this command line will be carried out with the Administrator privileges, including installation of software.

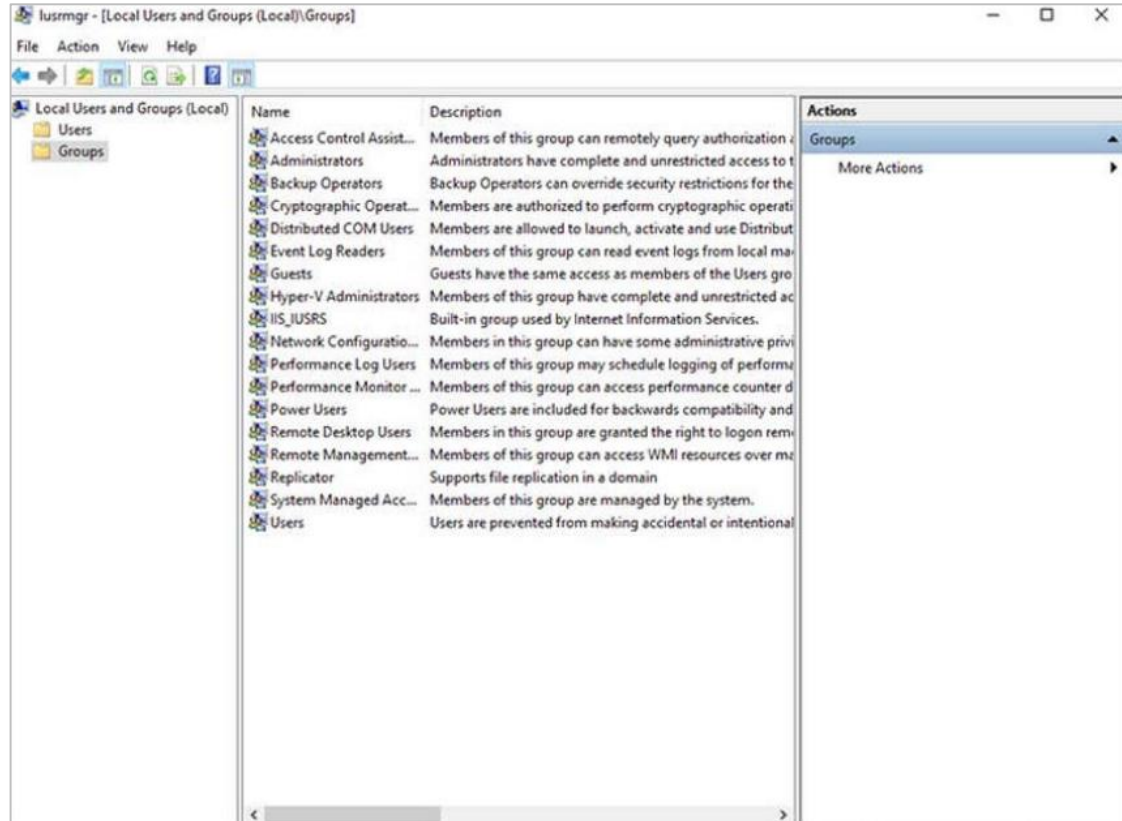


Local Users and Domains

- When a new computer is started for the first time, or Windows is installed, there will be a prompt to create a user account. This is known as a local user.
- This account contains all the customization settings, access permissions, file locations, and many other user-specific data.
- 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 into Windows that are used for specific tasks.

Local Users and Domains (Contd.)

- Local users and groups are managed with the `lusrmgr.msc` control panel applet, as shown in the figure.
- Windows 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.



CLI and PowerShell

- The Windows command line interface (CLI) can be used to run programs, navigate the file system, and manage files and folders.
- To open the Windows CLI, search for `cmd.exe` and click the program. 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. This followed by a colon and backslash (\).
 - Commands that have optional switches use the forward slash (/) to delineate between the command and the switch option.
 - You can use the Tab key to auto-complete commands when directories or files are referenced.
 - Windows keeps a history of the commands that were entered during a CLI session. Access previously entered commands by using the up and down arrow keys.
 - To switch between storage devices, type the letter of the device, followed by a colon, and then press Enter.

CLI and PowerShell (Contd.)

- 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.
- 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.

CLI and PowerShell (Contd.)

- To see more information about PowerShell and get started using it, type help, as shown in the command output.
- 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 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=188518.
    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 --
```

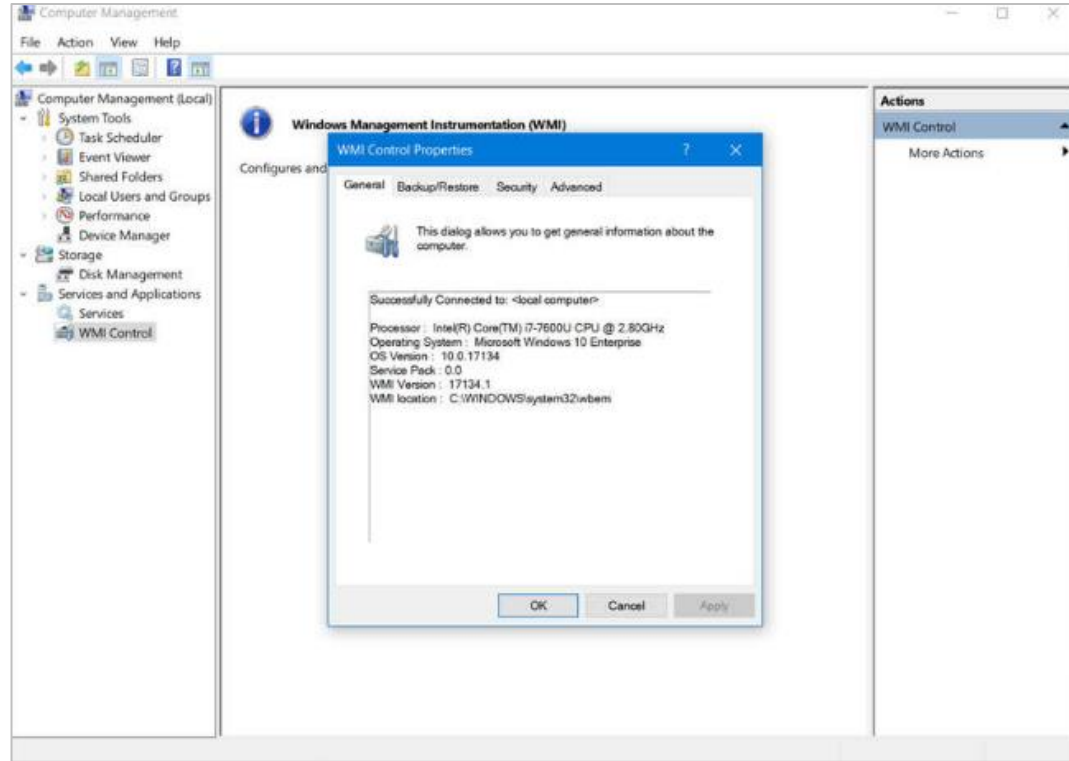
Windows Management Instrumentation

- **Windows Management Instrumentation (WMI)** is used to manage remote computers.
- It can retrieve information about computer components, hardware and software statistics, and monitor the health of remote computers.
- To open the WMI control from the Control Panel, double-click Administrative Tools > Computer Management to open the Computer Management window, expand the Services and Applications tree and right-click the WMI Control icon > Properties.

Windows Management Instrumentation

(Contd.)

- The WMI Control Properties window is shown in the figure. Four tabs in the WMI Control Properties window are:
 - 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



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 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:\>
```

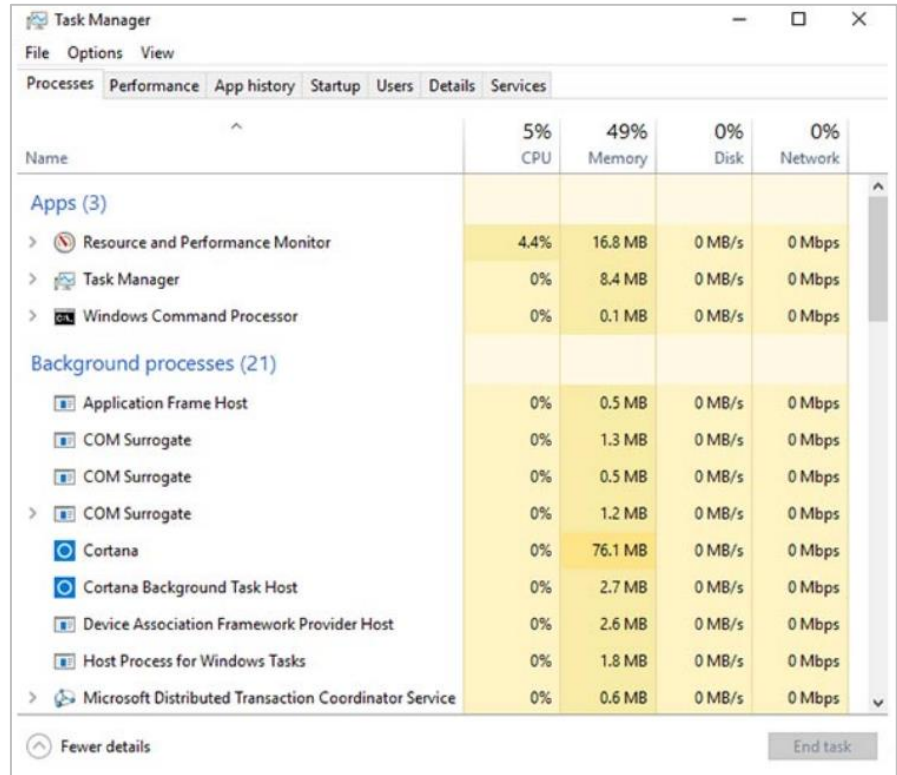
The net Command (Contd.)

- The following table lists some common net commands:

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

Task Manager and Resource Monitor

- There are two useful tools to help an administrator to understand the different applications, services, and processes that are running on a Windows computer.
- Task Manager
- The Task Manager, which is shown in the figure, provides a lot of information about the software that is running and the general performance of the computer.
- The Task Manager has seven tabs.



The screenshot shows the Windows Task Manager window with the Performance tab selected. The window title is 'Task Manager' and it has a menu bar with 'File', 'Options', and 'View'. Below the menu bar are seven tabs: 'Processes', 'Performance', 'App history', 'Startup', 'Users', 'Details', and 'Services'. The Performance tab is active, displaying a table of resource usage for various processes. The table has four columns: 'Name', 'CPU', 'Memory', 'Disk', and 'Network'. The CPU column shows 5% usage, Memory shows 49%, Disk shows 0%, and Network shows 0%. The table is divided into two sections: 'Apps (3)' and 'Background processes (21)'. The 'Apps (3)' section includes 'Resource and Performance Monitor' (4.4% CPU, 16.8 MB Memory), 'Task Manager' (0% CPU, 8.4 MB Memory), and 'Windows Command Processor' (0% CPU, 0.1 MB Memory). The 'Background processes (21)' section includes 'Application Frame Host' (0% CPU, 0.5 MB Memory), 'COM Surrogate' (0% CPU, 1.3 MB Memory), 'COM Surrogate' (0% CPU, 0.5 MB Memory), 'COM Surrogate' (0% CPU, 1.2 MB Memory), 'Cortana' (0% CPU, 76.1 MB Memory), 'Cortana Background Task Host' (0% CPU, 2.7 MB Memory), 'Device Association Framework Provider Host' (0% CPU, 2.6 MB Memory), 'Host Process for Windows Tasks' (0% CPU, 1.8 MB Memory), and 'Microsoft Distributed Transaction Coordinator Service' (0% CPU, 0.6 MB Memory). At the bottom of the window, there is a 'Fewer details' button on the left and an 'End task' button on the right.

Name	5% CPU	49% Memory	0% Disk	0% Network
Apps (3)				
> Resource and Performance Monitor	4.4%	16.8 MB	0 MB/s	0 Mbps
> Task Manager	0%	8.4 MB	0 MB/s	0 Mbps
> Windows Command Processor	0%	0.1 MB	0 MB/s	0 Mbps
Background processes (21)				
Application Frame Host	0%	0.5 MB	0 MB/s	0 Mbps
COM Surrogate	0%	1.3 MB	0 MB/s	0 Mbps
COM Surrogate	0%	0.5 MB	0 MB/s	0 Mbps
> COM Surrogate	0%	1.2 MB	0 MB/s	0 Mbps
Cortana	0%	76.1 MB	0 MB/s	0 Mbps
Cortana Background Task Host	0%	2.7 MB	0 MB/s	0 Mbps
Device Association Framework Provider Host	0%	2.6 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks	0%	1.8 MB	0 MB/s	0 Mbps
> Microsoft Distributed Transaction Coordinator Service	0%	0.6 MB	0 MB/s	0 Mbps

Task Manager and Resource Monitor (Contd.)

- The following table describes the seven tabs in the Task

TM Tabs	Description
Processes	<ul style="list-style-type: none">• Lists all of the programs and processes that are currently running.• Displays the CPU, memory, disk, and network utilization of each process.• The properties can be examined or ended if it is not behaving properly or has stalled.
Performance	<ul style="list-style-type: none">• A view of the performance statistics provides a 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	<ul style="list-style-type: none">• The use of resources by application over time provides insight into applications that are consuming more resources.• Click Options and Show history for all processes to see the history of every process that has run since the computer was started.
Startup	<ul style="list-style-type: none">• All the applications and services that start when the computer is booted are shown in this tab.• To disable a program from starting at startup, right-click the item and choose Disable.

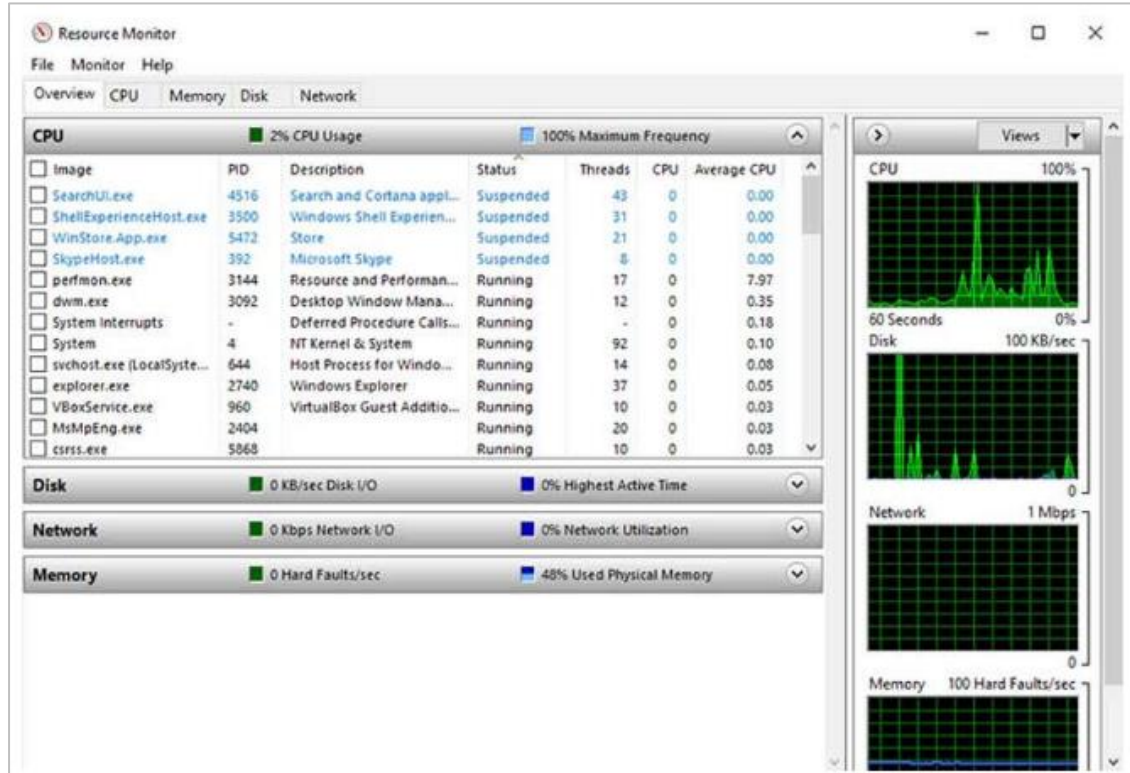
Task Manager and Resource Monitor (Contd.)

TM Tabs	Description
Users	<ul style="list-style-type: none">• All of the users that are logged on to the computer and all the resources that each user's applications and processes are using are shown in this tab.• From this tab, an administrator can disconnect a user from the computer.
Details	<ul style="list-style-type: none">• 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.• 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	<ul style="list-style-type: none">• All the services that are loaded are shown in this tab.• The process ID (PID) and a short description are also shown along with the status of either Running or Stopped.• At the bottom, there is a button to open the Services console which provides additional management of services.

Task Manager and Resource Monitor

(Contd.)

- Resource Monitor
- When more detailed information about resource usage is needed, the Resource Monitor can be used.
- When searching for the reason a computer may be acting erratically, the Resource Monitor can help to find the source of the problem.
- Resource Monitor has Five tabs.



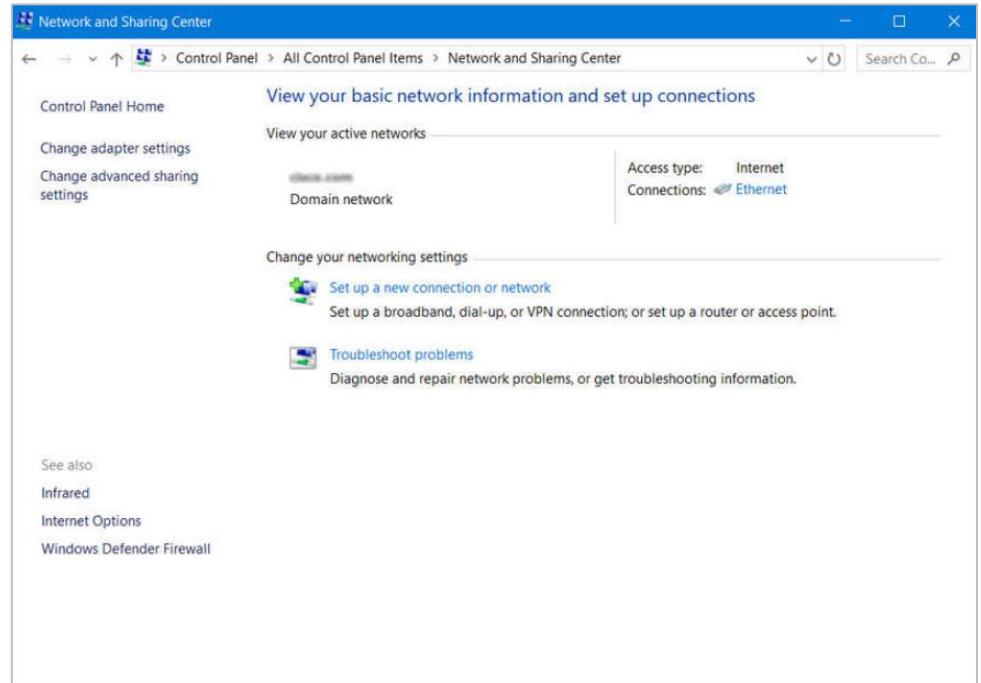
Task Manager and Resource Monitor (Contd.)

- The following table describes the five tabs:

RM Tabs	Description
Overview	The tab displays the general usage for each resource.
CPU	<ul style="list-style-type: none">• The PID, number of threads, which the process is using, and the average CPU usage of each process is shown.• Additional information about any services and the associated handles and modules can be seen by expanding the lower rows.
Memory	All the statistical information about how each process uses memory is shown in this tab and an overview of usage of all the RAM is shown below the Processes row.
Disk	All the processes that are using a disk are shown in this tab, with read/write statistics and an overview of each storage device.
Network	<ul style="list-style-type: none">• All the processes that are using the network are shown in this tab, with read/write statistics.• It is very useful when trying to determine which applications and processes are communicating over the network. Also, tell if an unauthorized process is accessing the network.

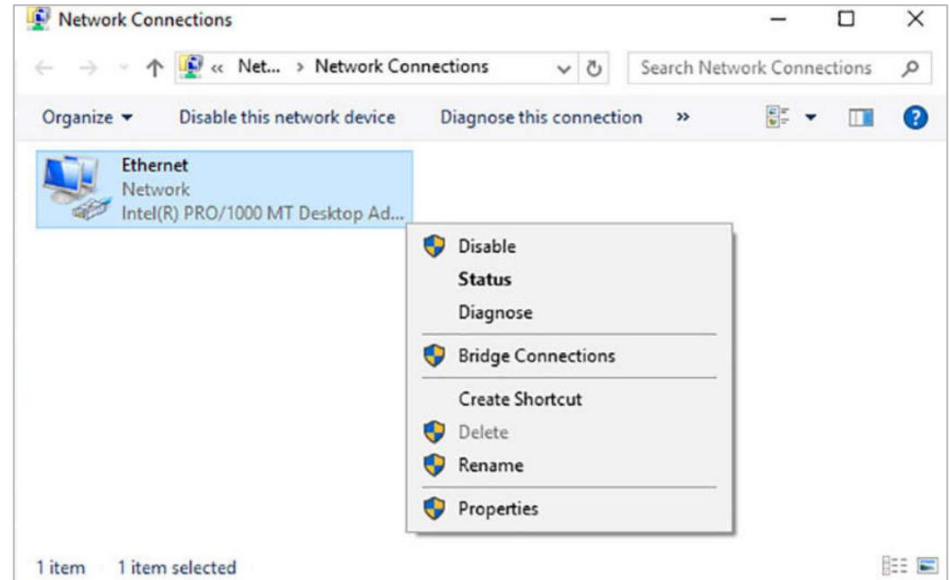
Networking

- 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.
- **Network and Sharing Center**
 - It is used to verify or create network connections, configure network sharing, and change network adapter settings.
 - The initial view shows an overview of the active network.
 - From the window, you can see the HomeGroup the computer belongs to, or create one if it is not already part of a HomeGroup. Note that HomeGroup was removed from Windows 10 in version 1803.



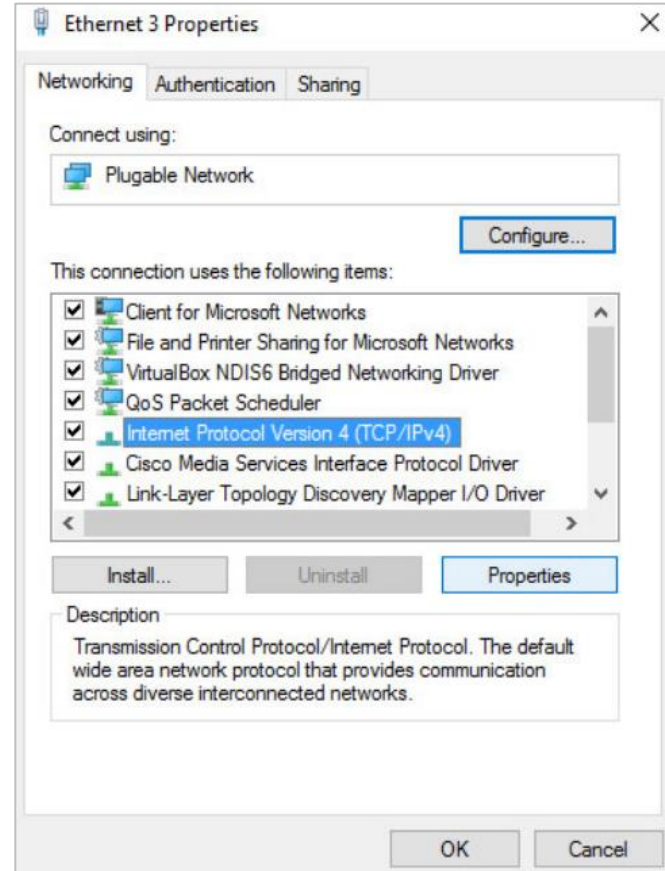
Networking (Contd.)

- Change Adapter Settings
- To configure a network adapter, choose Change adapter settings in the Networking and Sharing Center to show all of the network connections that are available. Select the adapter that is to be configured.
- Following are the steps to change an Ethernet adapter to acquire its IPv4 address automatically from the network:
 - Step 1: Access Adaptor Properties
 - Right-click the adapter you wish to configure and choose Properties, as shown in the figure.



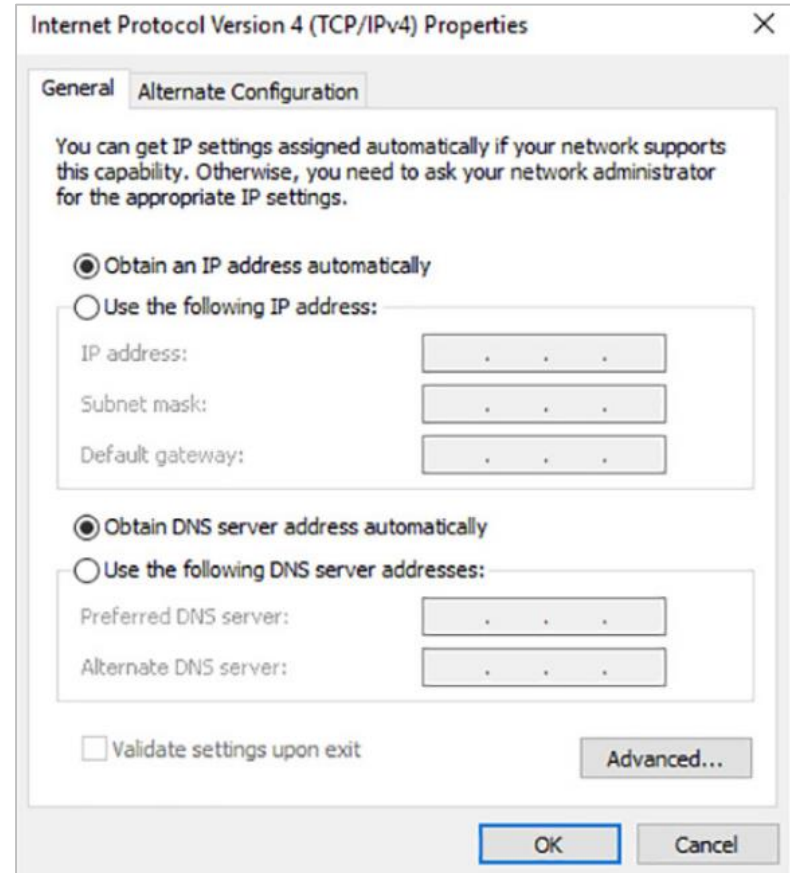
Networking (Contd.)

- Step 2: Access TCP/IPv4 properties
- This connection uses Internet Protocol Version 4 (TCP/IPv4) or Internet Protocol Version 6 (TCP/IPv6) depending on which version the user wish to use.
- In the figure, IPv4 is being selected.



Networking (Contd.)

- Step 3: Change Settings
- Click Properties to configure the adapter.
- In the Properties dialogue box, choose to Obtain an address automatically if there is a DHCP server available on the network or if the user wish to configure addressing manually, fill in the address, subnet, default gateway, and DNS servers.
- 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.



Networking (Contd.)

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

```
Command Prompt - nslookup
C:\Users\rsanchez>nslookup
Default Server: UnKnown
Address: 10.2.0.1

> set debug
> wikipedia.org
Server: UnKnown
Address: 10.2.0.1

-----
Got answer:
HEADER:
    opcode = QUERY, id = 2, rcode = NOERROR
    header flags: response, want recursion, recursion avail.
    questions = 1, answers = 1, authority records = 0, additional = 0

QUESTIONS:
    wikipedia.org, type = A, class = IN
ANSWERS:
-> wikipedia.org
    internet address = 208.80.153.224
    ttl = 600 (10 mins)

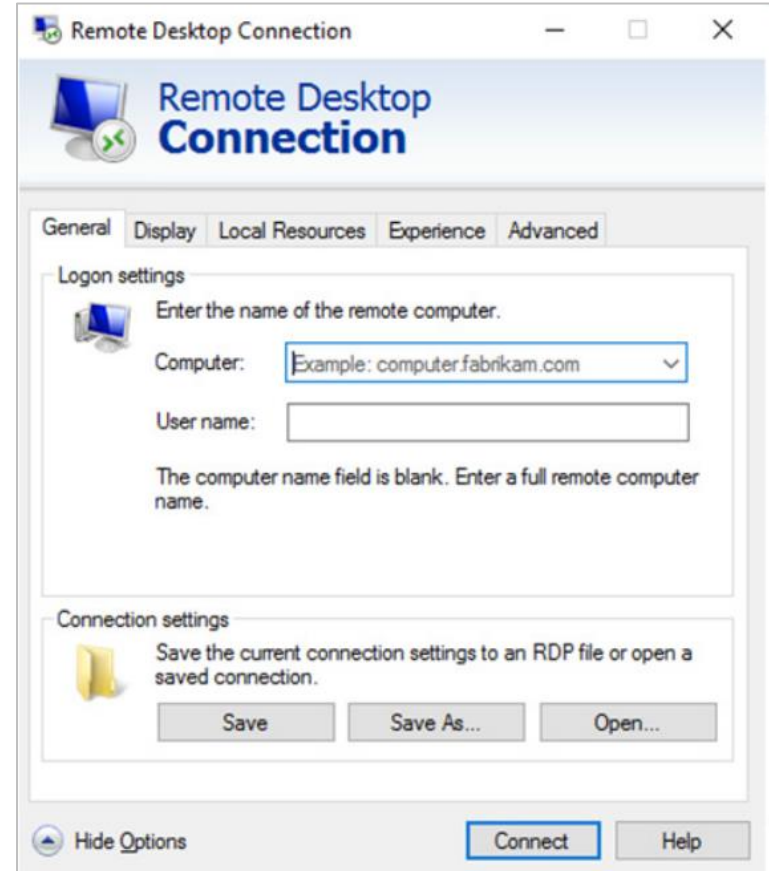
-----
Non-authoritative answer:
```

Accessing Network Resources

- Windows uses networking for many different applications such as web, email, and file services.
- 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.
- In the UNC, servername is the server that is hosting the resource. 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.
- 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 files to restrict users and groups to specific functions.
- There are also special shares that are automatically created by Windows. These shares are called administrative shares and are identified by a dollar sign (\$) that comes after the share name.

Accessing Network Resources (Contd.)

- Besides accessing shares on remote hosts, the user can also log in to a remote host and manipulate that computer, as if it were local, to make configuration changes, install software, or troubleshoot an issue.
- In Windows, this feature uses the Remote Desktop Protocol (RDP). The Remote Desktop Connection window is shown in the figure.
- Since Remote Desktop Protocol (RDP) is designed to permit remote users to control individual hosts, it is a natural target for threat actors.



Windows Server

- Most Windows installations are performed as desktop installations on desktops and laptops.
- There is another edition of Windows that is mainly used in data centers called Windows Server. This is a family of Microsoft products that began with Windows Server 2003.
- Windows Server hosts many different services and can fulfill different roles within a company.
- These are some of the services that Windows Server provides:
 - Network Services: DNS, DHCP, Terminal services, Network Controller, and Hyper-V Network virtualization
 - File Services: SMB, NFS, and DFS
 - Web Services: FTP, HTTP, and HTTPS
 - Management: Group policy and Active Directory domain services control
- **Note:** *Although there is a Windows Server 2000, it is considered a client version of Windows NT 5.0. Windows Server 2003 is a server based on NT 5.2 and begins a new family of Windows Server versions.*

Windows Configuration and Monitoring

Lab - Create User Accounts

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

Windows Configuration and Monitoring

Lab - Using Windows PowerShell

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

Windows Configuration and Monitoring

Lab - Windows Task Manager

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

Lab - Monitor and Manage System

Resources in Windows

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

3.4 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.
- By examining these connections, it is possible to determine the programs which are listening for connections that are not authorized.
- When a program is suspected of being malware, the process can be shut down with Task Manager, and malware removal software can be used to clean the computer.
- To make this process easier, the connections can be linked to the running processes that were created by them in Task Manager.

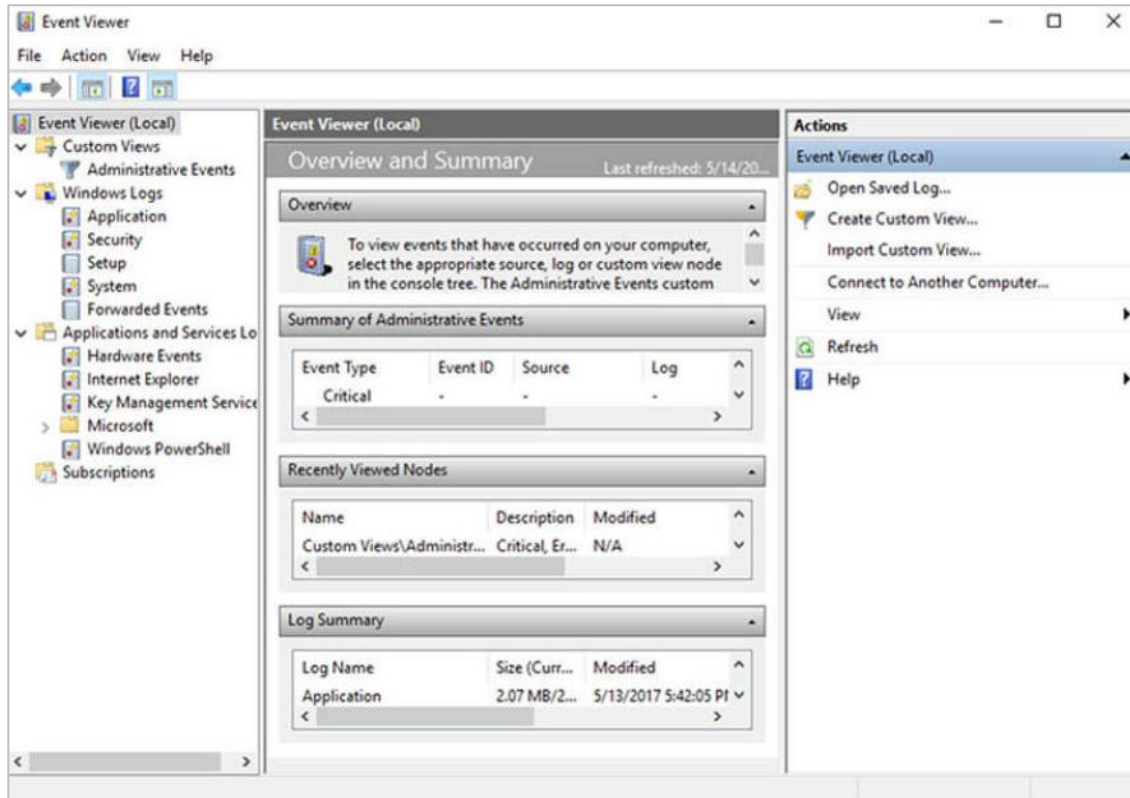
The netstat Command (Contd.)

- To do this, open a command prompt with administrative privileges and enter the `netstat -abno` command.
- 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.
- There may be more than one process listed with the same name. If this is the case, use the unique PID to find the correct process. To display the PIDs for the processes in the Task Manager, open the Task Manager, right-click the table heading and select PID.

```
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
```

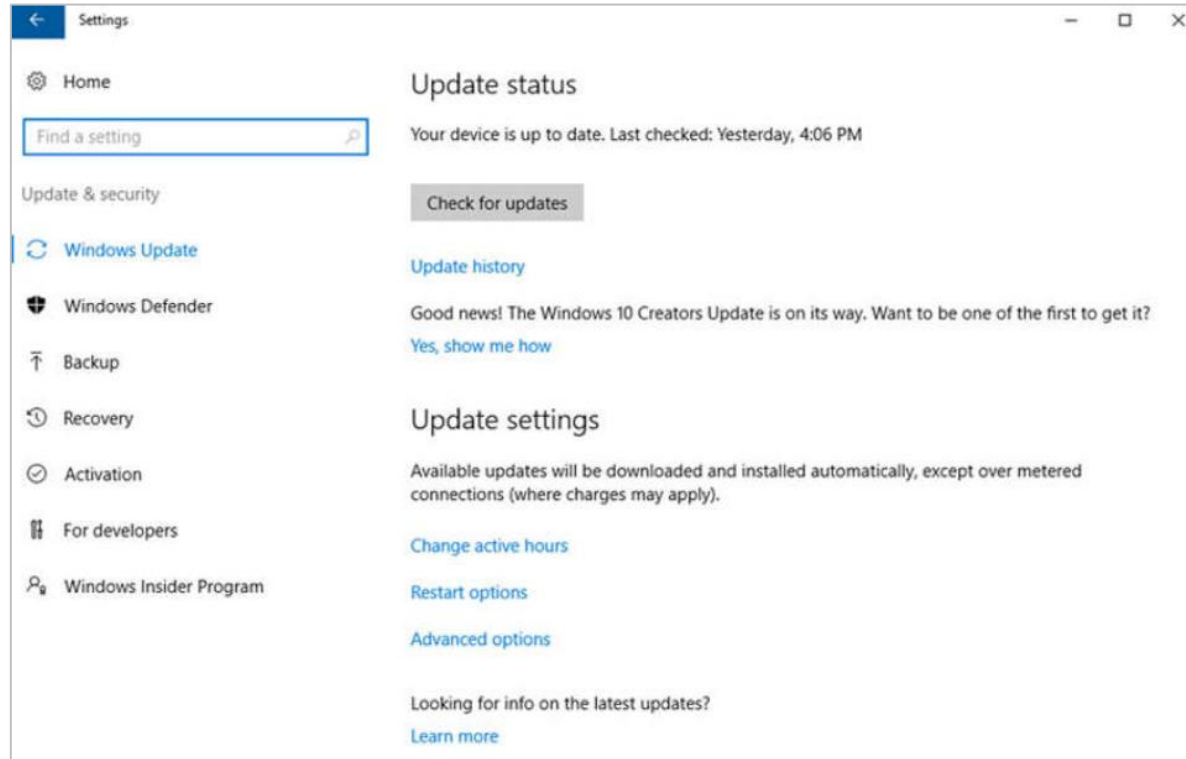
Event Viewer

- Windows Event Viewer logs the history of application, security, and system events.
- These log files are a troubleshooting tool as they provide information necessary to identify a problem.
- 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 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 the attacks, always ensure Windows is up to date with the latest service packs and security patches.
- Update status, shown in the figure, allows you to check for updates manually and see the update history of the computer.
- Patches are code updates that manufacturers provide to prevent a newly discovered virus or worm from making a successful attack.

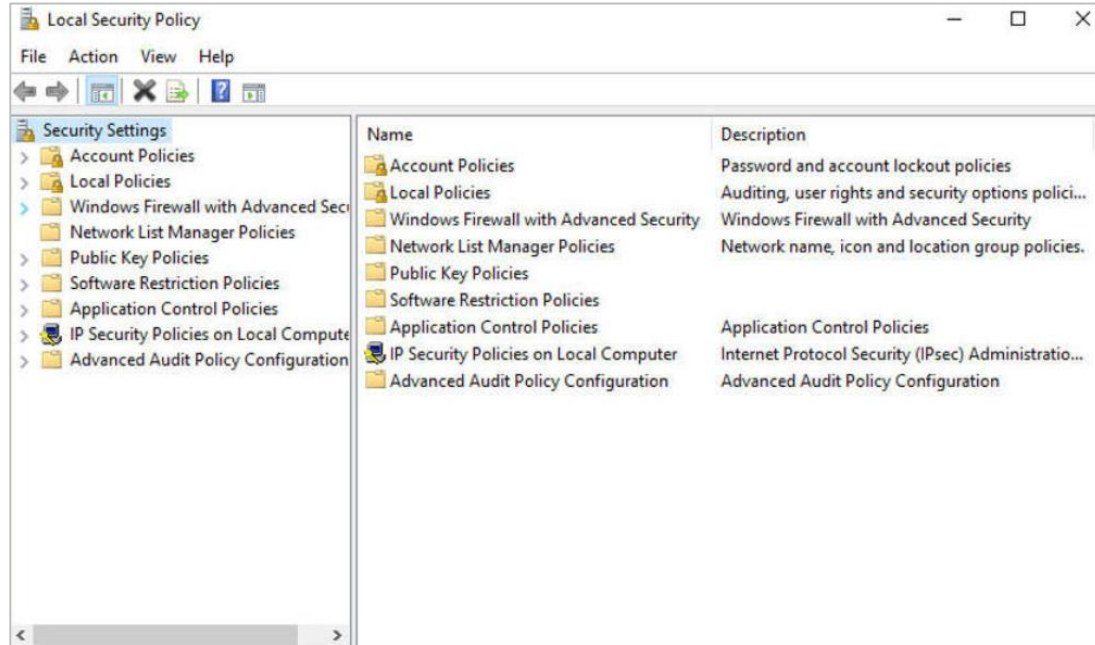


Windows Update Management (Contd.)

- 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.
- It is highly desirable that enterprises utilize systems that automatically distribute, install, and track security updates.
- Windows routinely checks the Windows Update website for high-priority updates that can help protect a computer from the latest security threats.
- There are also settings for the hours where the computer will not automatically restart, for example during regular business hours.
- Advanced options are also available to choose how updates are installed how other Microsoft products are updated.

Local Security Policy

- A security policy is a set of objectives that ensures the security of a network, the data, and the computer systems in an organization.
- In most networks that use Windows computers, Active Directory is configured with Domains on a Windows Server. Windows computers join the domain.
- Windows Local Security Policy can be used for stand-alone computers that are not part of an Active Directory domain.



Local Security Policy (Contd.)

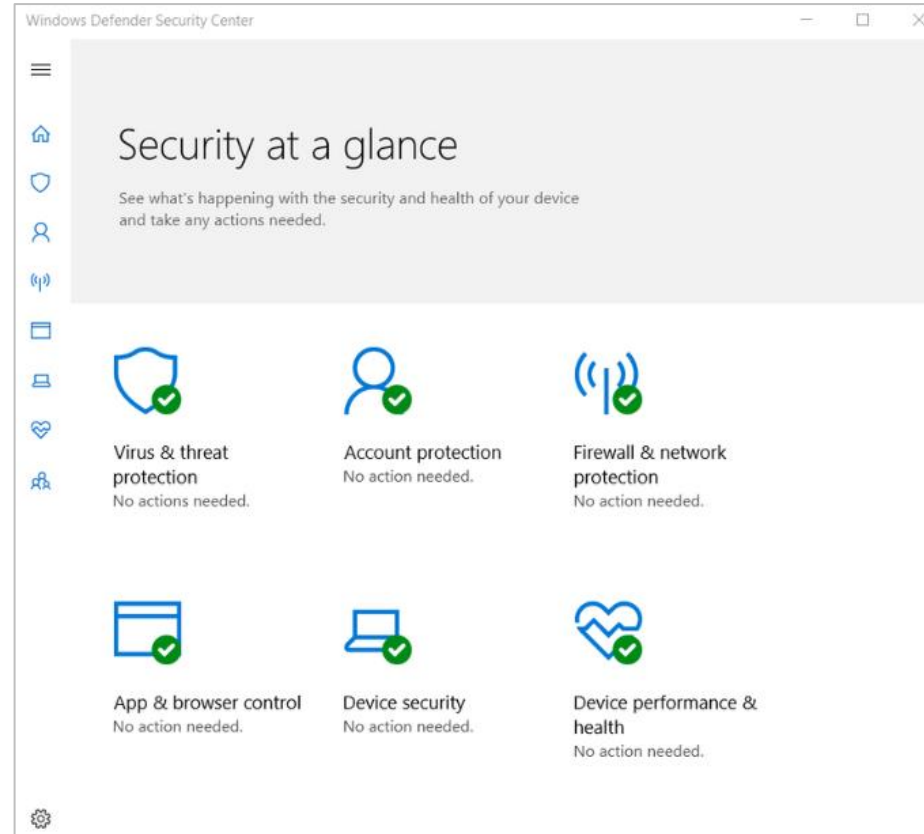
- Password guidelines are an important component of a security policy.
- In the Local Security Policy, Password Policy is found under Account Policies and defines the criteria for the passwords for all of the users on the local computer.
- Use the Account Lockout Policy in Account Policies to prevent brute-force login attempts.
- It is important to ensure 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.
- If the Local Security Policy on every stand-alone computer is the same, then use the Export Policy feature. 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 security settings that apply specifically to the local computer. The user can configure User Rights, Firewall Rules, and the ability to restrict the files that users or groups are allowed to run with the AppLocker.

Windows Defender

- Malware includes viruses, worms, Trojan horses, keyloggers, spyware, and adware. These are designed to invade privacy, steal information, damage the computer, or corrupt data.
- It is important to 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 the 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 about unsafe programs about to be installed or unsafe websites.

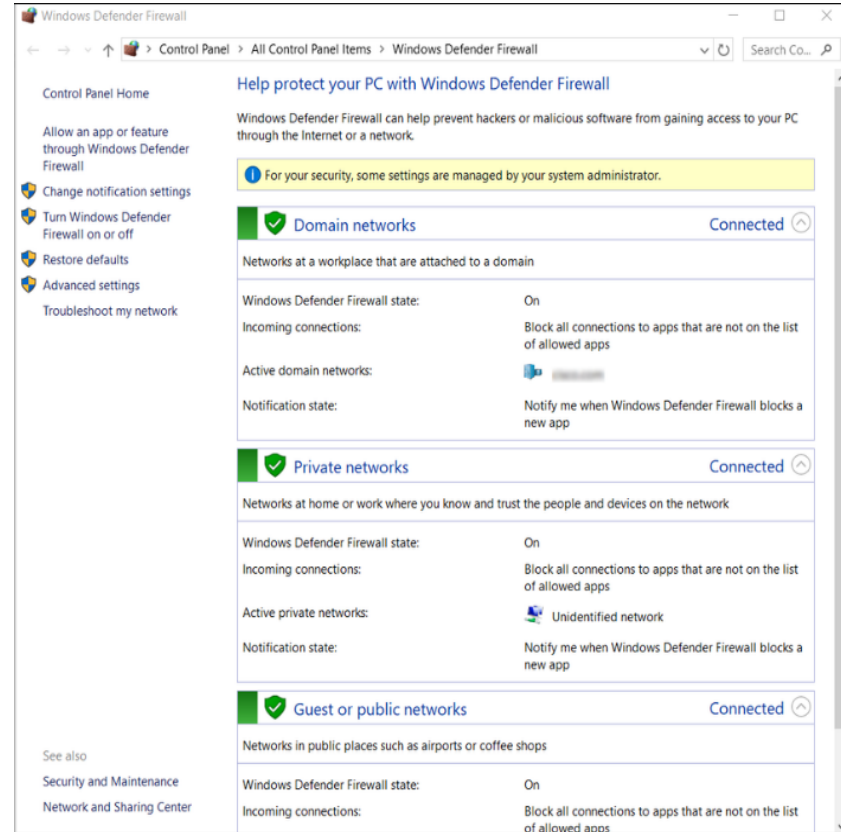
Windows Defender (Contd.)

- It may take multiple scans to completely remove all malicious software. Run only one malware protection program at a time.
- Several 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.
- 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.



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.



Thank you! Questions?



Vladimír Veselý

updated: 2023-02-14

<https://www.fit.vutbr.cz/research/groups/nes@fit>

Module 4: Linux Overview

Instructor Materials

CyberOps Associate v1.0

Module 4: Linux Overview

Module Objectives

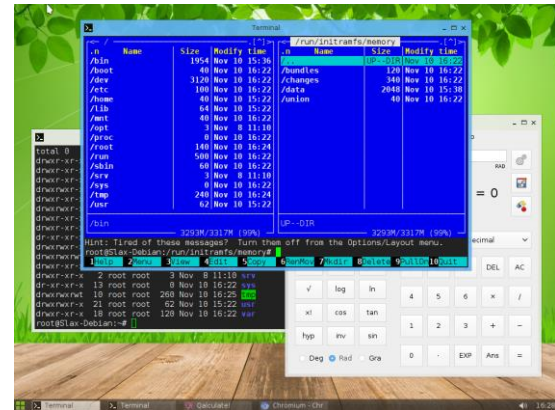
- Module Title: Linux Overview
- Module Objective: Implement basic Linux security.

Topic Title	Topic Objective
Linux Basics	Explain why Linux skills are essential for network security monitoring and investigation.
Working in the Linux Shell	Use the Linux shell to manipulate text files.
Linux Servers and Clients	Explain how client-server networks function.
Basic Server Administration	Explain how a Linux administrator locates and manipulates security log files.
The Linux File System	Manage the Linux file system and permissions.
Working in the Linux GUI	Explain the basic components of the Linux GUI.
Working on a Linux Host	Use tools to detect malware on a Linux host.

4.1 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.
- Sguil is the cybersecurity analyst console in a special version of Linux called Security Onion.
- Security Onion is an open source suite of tools that work together for network security analysis.

The screenshot displays the Sguil-0.9.0 interface, which is a cybersecurity analyst console. The main window shows a list of network events under the 'Escalated Events' tab. The events are organized in a table with columns for status (ST), count (CNT), sensor, alert ID, date/time, source IP (Src IP), source port (SPort), destination IP (Dst IP), destination port (DPort), priority (Pr), and event message. Several events are highlighted in yellow, indicating they are of interest.

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	7	seconion...	5.1583	2020-05-10 21:29:13	209.165.201.17	52458	209.165.200.235	80	6	ET INFO Dotted Quad Host HTA
RT	7	seconion...	5.1584	2020-05-10 21:29:13	209.165.201.17	52458	209.165.200.235	80	6	ET POLICY Possible HTA Applica...
RT	1	seconion...	5.1599	2020-05-10 21:29:13	209.165.201.17	52460	209.165.200.235	80	6	ET TROJAN Probable OneLoudner ...
RT	1	seconion...	5.1600	2020-05-10 21:29:13	209.165.201.17	52468	209.165.200.235	80	6	ET WEB_SERVER Possible Cher...
RT	7	seconion...	7.1896	2020-05-10 21:29:13	209.165.201.17	52458	209.165.200.235	80	6	ET INFO Dotted Quad Host HTA ...
RT	7	seconion...	7.1897	2020-05-10 21:29:13	209.165.201.17	52458	209.165.200.235	80	6	ET POLICY Possible HTA Applica...
RT	1	seconion...	7.1912	2020-05-10 21:29:13	209.165.201.17	52460	209.165.200.235	80	6	ET TROJAN Probable OneLoudner ...
RT	1	seconion...	7.1913	2020-05-10 21:29:13	209.165.201.17	52468	209.165.200.235	80	6	ET WEB_SERVER Possible Cher...
RT	1	seconion...	5.1679	2020-05-10 21:29:49	209.165.201.17	52836	209.165.200.235	80	6	ET WEB_SERVER /bin/bash In U...
RT	1	seconion...	7.1992	2020-05-10 21:29:49	209.165.201.17	52836	209.165.200.235	80	6	ET WEB_SERVER /bin/bash In U...
RT	49	seconion...	7.1998	2020-05-10 21:29:52	209.165.201.17	52896	209.165.200.235	80	6	ET WEB_SERVER /bin/sh In URI ...
RT	49	seconion...	5.1701	2020-05-10 21:29:52	209.165.201.17	52896	209.165.200.235	80	6	ET WEB_SERVER /bin/sh In URI ...
RT	1	seconion...	5.1770	2020-05-10 21:41:13	209.165.201.17	38782	209.165.200.235	3306	6	ET SCAN Suspicious inbound to ...

The bottom panel of the interface shows a detailed view of a packet capture. The 'System Msgs' tab is selected, displaying a list of system messages. The selected message is a TCP packet from 209.165.201.17 to 209.165.200.235 on port 80. The packet details are shown in a table format, including source and destination IP, port, and sequence number. The packet data is displayed in hexadecimal and ASCII format, showing a GET request for a file named /11 HTTP/1.1.

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
TCP	209.165.201.17	209.165.200.235	4	5	0	172	50175	2	0	63	16900

The packet data is shown in hexadecimal and ASCII format, including the sequence number (2237277941), acknowledgment number (1593194311), and the request body (GET /11 HTTP/1.1).

Linux in the SOC (Contd.)

- The following table lists a few tools that are often found in a SOC:

SOC Tool	Description
Network packet capture software	<ul style="list-style-type: none">• A crucial tool for a SOC analyst as it makes it possible to observe and understand every detail of a network transaction.• Wireshark is a popular packet capture tool.
Malware analysis tools	<ul style="list-style-type: none">• These tools allow analysts to safely run and observe malware execution without the risk of compromising the underlying system.
Intrusion detection systems (IDSs)	<ul style="list-style-type: none">• These tools are used for real-time traffic monitoring and inspection.• If any aspect of the currently flowing traffic matches any of the established rules, a pre-defined action is taken.

Linux in the SOC (Contd.)

SOC Tool	Description
Firewalls	<ul style="list-style-type: none">• This software is used to specify, based on pre-defined rules, whether traffic is allowed to enter or leave a network or device.
Log managers	<ul style="list-style-type: none">• Log files are used to record events.• Because a network can generate a very large number of log entries, log manager software is employed to facilitate log monitoring.
Security information and event management (SIEM)	<ul style="list-style-type: none">• SIEMs provide real-time analysis of alerts and log entries generated by network appliances such as IDSs and firewalls.
Ticketing systems	<ul style="list-style-type: none">• Task ticket assignment, editing, and recording is done through a ticket management system. Security alerts are often assigned to analysts through a ticketing system.

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.



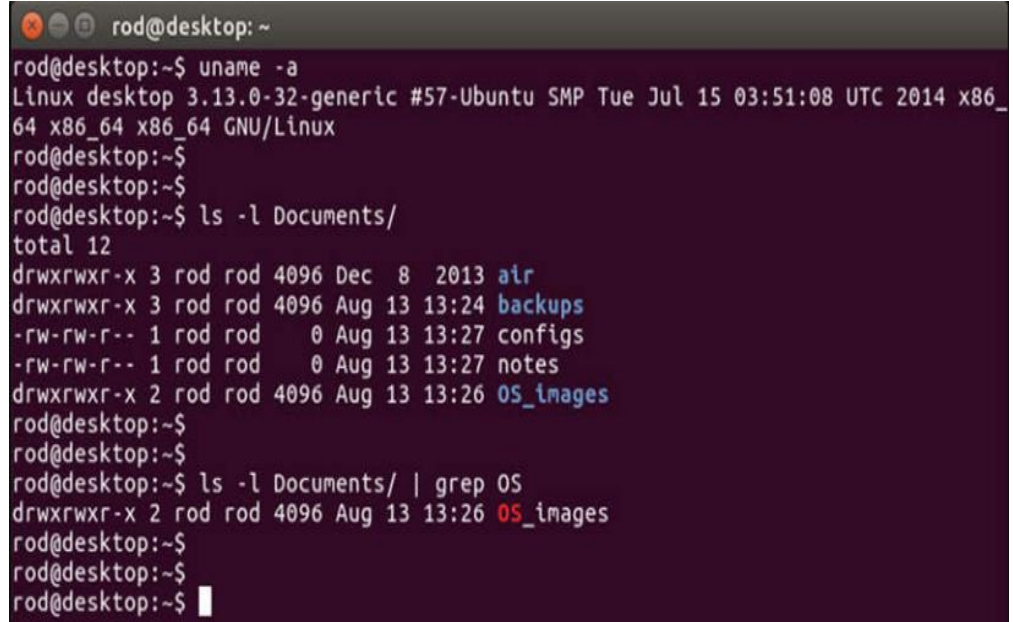
4.2 Working in the Linux Shell

The Linux Shell

- In Linux, the user communicates with the OS by using the CLI or the GUI.
- Linux often starts in the GUI by default. This hides the CLI from the user.
- One way to access the CLI from the GUI is through a terminal emulator application. These applications provide user access to the CLI and are named as some variation of the word terminal.
- In Linux, 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.
- **Note:** *The terms shell, console, console window, CLI terminal, and terminal window are often used interchangeably.*

The Linux Shell (Contd.)

- The figure shows *gnome-terminal*, a popular Linux terminal emulator.



```
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

- Linux commands are programs created to perform a specific task.
- As the commands are programs stored on the disk, when a user types a command, the shell must find it on the disk before it can be executed.
- The following table lists basic Linux commands and their functions:

Command	Description
mv	Moves or renames files and directories.
chmod	Modifies file permissions.
chown	Changes the ownership of a file.
dd	Copies data from an input to an output.
pwd	Displays the name of the current directory.
ps	Lists the processes that are currently running in the system.
su	Simulates a login as another user or to become a superuser.

Basic Commands (Contd.)

Command	Description
sudo	Runs a command as a super user, by default, or another named user.
grep	Used to search for specific strings of characters within a file or other command outputs.
ifconfig	Used to display or configure network card related information.
apt-get	Used to install, configure and remove packages on Debian and its derivatives.
iwconfig	Used to display or configure wireless network card related information.
shutdown	Shuts down the system and performs shut down related tasks including restart, halt, put to sleep or kick out all currently connected users.
passwd	Used to change the password.
cat	Used to list the contents of a file and expects the file name as the parameter.
man	Used to display the documentation for a specific command.

File and Directory Commands

- Many command line tools are included in Linux by default. The following table lists a few of the most common commands related to files and directories:

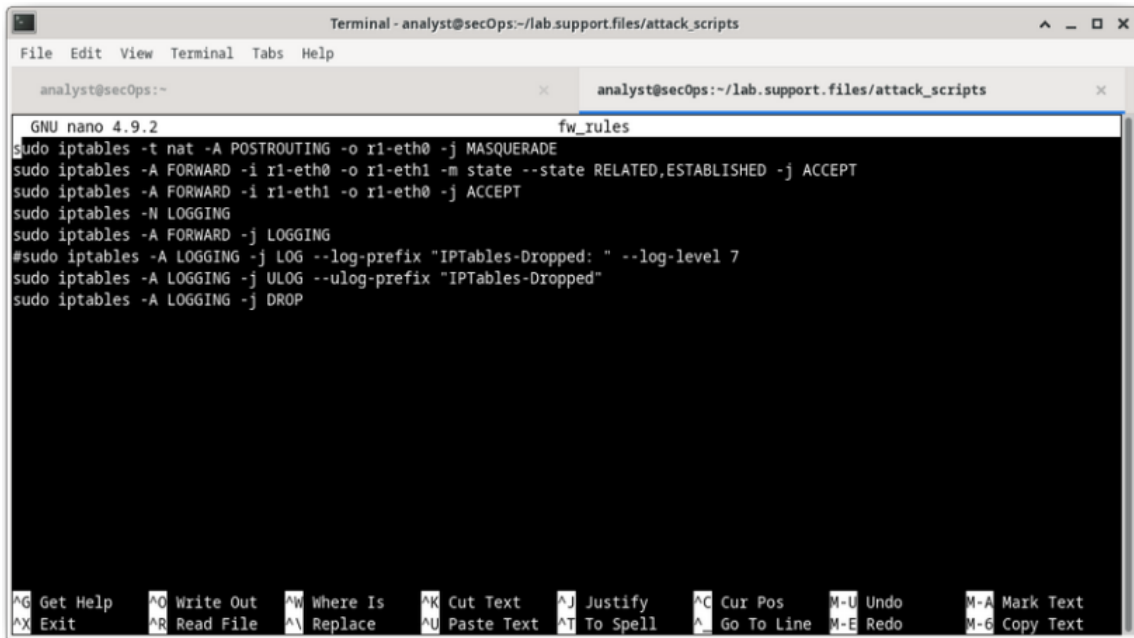
Command	Description
ls	Displays the files inside a directory.
cd	Changes the current directory.
mkdir	Creates a directory under the current directory.
cp	Copies files from source to destination.
mv	Moves files to a different directory.
rm	Removes files.
grep	Searches for specific strings of characters within a file or other commands outputs.
cat	Lists the contents of a file and expects the file name as the parameter.

Working with Text Files

- Linux has many different text editors, with various features and functions.
- Some text editors include graphical interfaces while others are command-line only tools. Each text editor includes a feature set designed to support a specific type of task.
- Some text editors focus on the programmer and include features such as syntax highlighting, parenthesis check, and other programming-focused features.
- While graphical text editors are convenient and easy to use, command line-based text editors are very important for Linux users. The main benefit of command-line-based text editors is that they allow for text file editing from a remote computer.

Working with Text Files (Contd.)

- The figure shows nano, a popular command-line text editor.
- The administrator is editing firewall rules. Text editors are often used for system configuration and maintenance in Linux.
- Due to the lack of graphical support, nano (or GNU nano) can only be controlled with the keyboard.



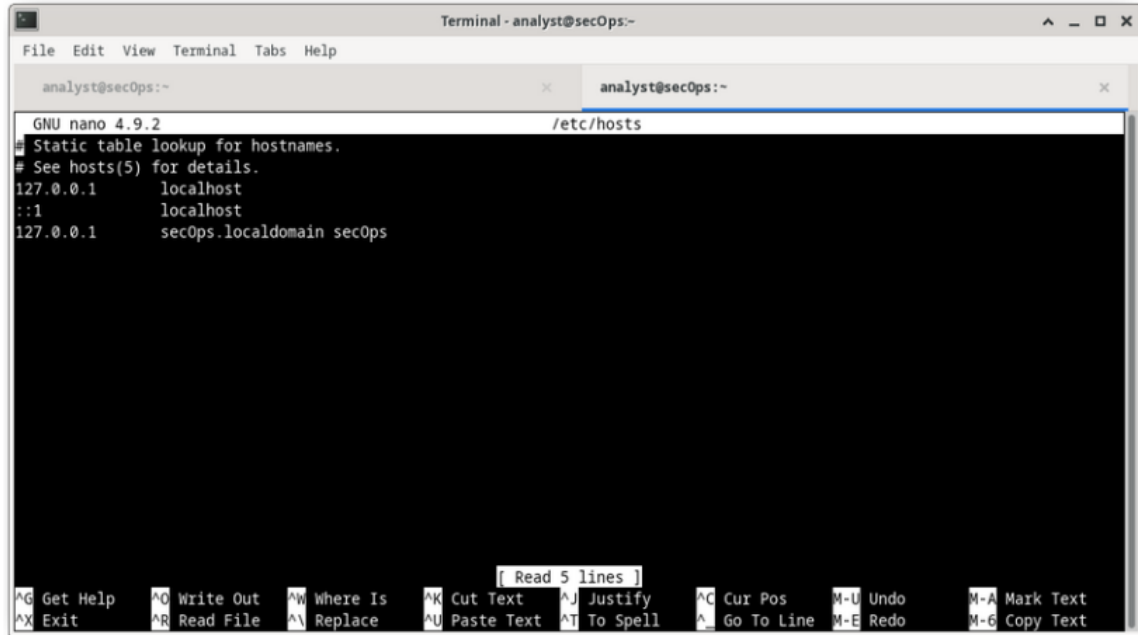
```
Terminal - analyst@secOps:~/lab.support.files/attack_scripts
File Edit View Terminal Tabs Help
analyst@secOps:~
analyst@secOps:~/lab.support.files/attack_scripts
GNU nano 4.9.2 fw_rules
sudo iptables -t nat -A POSTROUTING -o r1-eth0 -j MASQUERADE
sudo iptables -A FORWARD -i r1-eth0 -o r1-eth1 -m 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 ^N Replace ^U Paste Text ^I To Spell ^_ Go To Line M-E Redo M-G 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, and the directories.
- Configuration files are text files which are used to store adjustments and settings for specific applications or services.
- Users with proper permission levels can use text editors to change the contents of configuration files.
- After the changes are made, the file is saved and can be used by the related service or application. Users are able to specify exactly how they want any given application or service to behave. When launched, services and applications check the contents of specific configuration files to adjust their behavior accordingly.
- **Note:** *The administrator used the command **sudo nano /etc/hosts** to open the file. The command **sudo** (short for “superuser do”) invokes the superuser privilege to use the nano text editor to open the host file.*

The Importance of Text Files in Linux (Contd.)

- In the figure, the administrator opened the host configuration file in nano for editing.
- The host file contains static mappings of host IP addresses to names.
- The names serve as shortcuts that allow connecting to other devices by using a name instead of an IP address. Only the superuser can change the host file.



```
Terminal - analyst@secOps--
File Edit View Terminal Tabs Help
analyst@secOps:~
analyst@secOps:~
GNU nano 4.9.2 /etc/hosts
# Static table lookup for hostnames.
# See hosts(5) for details.
127.0.0.1 localhost
::1 localhost
127.0.0.1 secOps.localdomain secOps
[ Read 5 lines ]
^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-G Copy Text
```

Lab – Working with Text Files in the CLI

- In this lab, you will get familiar with Linux command-line text editors and configuration files.

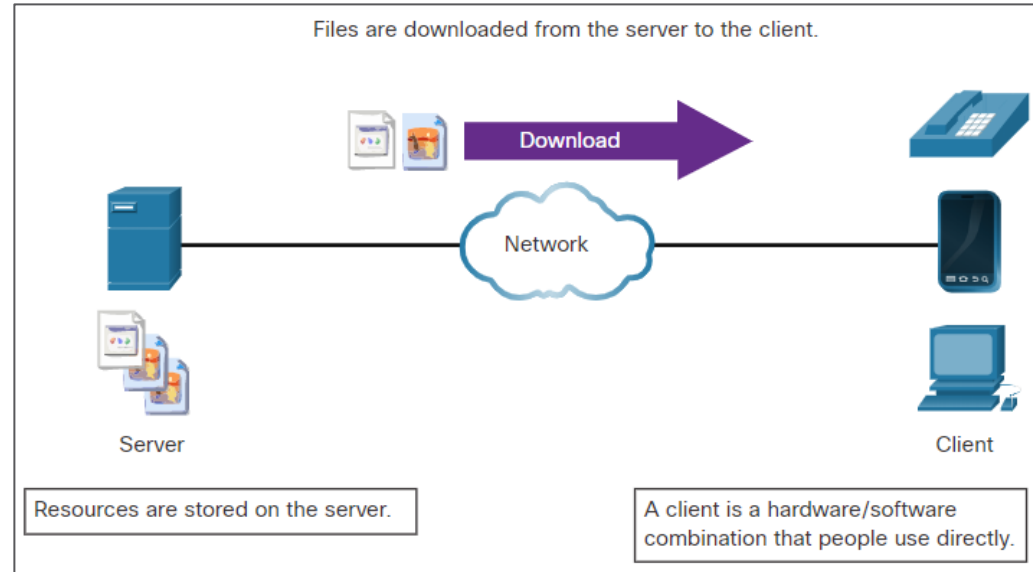
Lab – Getting Familiar with the Linux Shell

- In this lab, you will use the Linux command line to manage files and folders and perform some basic administrative tasks.

4.3 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.
- The following table lists a few commonly used ports and their services. These are also called as well-known ports.

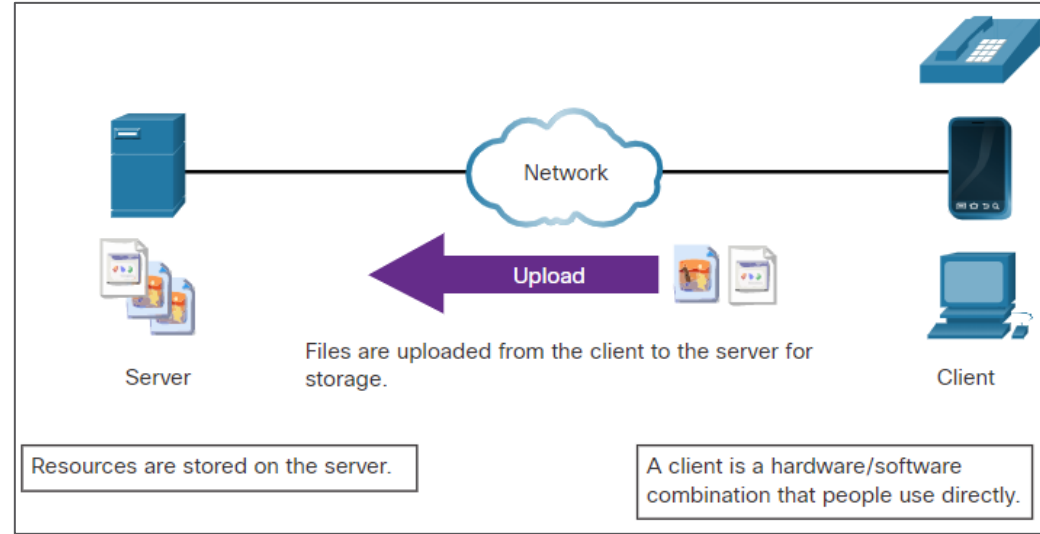
Port	Description
20/21	File Transfer Protocol (FTP)
22	Secure Shell (SSH)
23	Telnet remote login service
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
67/68	Dynamic Host Configuration Protocol (DHCP)

Servers, Services, and Their Ports (Contd.)

Port	Description
69	Trivial File Transfer Protocol (TFTP)
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.



Lab - Linux Servers

- In this lab, you will use the Linux command line to identify servers that are running on a computer.

4.4 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;
```

Service Configuration Files (Contd.)

- The command output shows the configuration file for the network time protocol (NTP).

```
[analyst@secOps ~]$ cat /etc/ntp.conf
# Please consider joining the pool:
#
#       http://www.pool.ntp.org/join.html
#
# For additional information see:
# - https://wiki.archlinux.org/index.php/Network_Time_Protocol_daemon
# - http://support.ntp.org/bin/view/Support/GettingStarted
# - the ntp.conf man page
# Associate to Arch's NTP pool
server 0.arch.pool.ntp.org
server 1.arch.pool.ntp.org
server 2.arch.pool.ntp.org
server 3.arch.pool.ntp.org
# By default, the server allows:
# - all queries from the local host
# - only time queries from remote hosts, protected by rate limiting and kod
restrict default limited nomodify nopeer noquery notrap
restrict 127.0.0.1
restrict ::1
# Location of drift file
[analyst@secOps ~]$
```

Service Configuration Files (Contd.)

- The command output shows the configuration file for Snort, a Linux-based intrusion detection system (IDS).
- There is no rule for a configuration file format. It is the choice of the service's developer. However, the option = value format is often used.

```
[analyst@secOps ~]$ cat /etc/snort/snort.conf
#-----
#   VRT Rule Packages Snort.conf
#
#   For more information visit us at:
#   http://www.snort.org                Snort Website
#   http://vrt-blog.snort.org/         Sourcefire VRT Blog
#
#   Mailing list Contact:  snort-sigs@lists.sourceforge.net
#   False Positive reports: fp@sourcefire.com
#   Snort bugs:           bugs@snort.org
#
#   Compatible with Snort Versions:
#   VERSIONS : 2.9.9.0
#
#   Snort build options:
#   OPTIONS : --enable-gre --enable-mpls --enable-targetbased --enable-ppm --enable-perfprofiling --
enable-zlib --enable-active-response --enable-normalizer --enable-reload --enable-react --enable-
flexresp3
<output omitted>
#####
# Step #1: Set the network variables.  For more information, see README.variables
#####
# Setup the network addresses you are protecting
##ipvar HOME_NET any
##ipvar HOME_NET [192.168.0.0/24,192.168.1.0/24]
ipvar HOME_NET [209.165.200.224/27]
# Set up the external network addresses.  Leave as "any" in most situations
ipvar EXTERNAL_NET any
```

Hardening Devices

- Device hardening involves implementing proven methods of securing the device and protecting its administrative access.
- Some of these methods involve maintaining passwords, configuring enhanced remote login features, and implementing secure login with SSH.
- Depending on the Linux distribution, many services are enabled by default. Stopping such services and ensuring they do not automatically start at boot time is another device hardening technique.
- OS updates are extremely important to maintaining a hardened device. OS developers create and issue fixes and patches regularly.

Hardening Devices (Contd.)

- 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
- Some logs contain information about daemons that are running in Linux. A daemon is a background process that runs without the need for user interaction.

Monitoring Service Logs (Contd.)

- The following table lists a few popular Linux log files and their functions:

Linux Log File	Description
<code>/var/log/messages</code>	<ul style="list-style-type: none">• This directory contains generic computer activity logs.• It is mainly used to store informational and non-critical system messages.
<code>/var/log/auth.log</code>	<ul style="list-style-type: none">• This file stores all authentication-related events in Debian and Ubuntu computers.• Anything involving the user authorization mechanism can be found in this file.
<code>/var/log/secure</code>	<ul style="list-style-type: none">• This directory is used by RedHat and CentOS computers.• It also tracks sudo logins, SSH logins, and other errors logged by SSSD.
<code>/var/log/boot.log</code>	<ul style="list-style-type: none">• This file stores boot-related information and messages logged during the computer startup process.

Monitoring Service Logs (Contd.)

Linux Log File	Description
<code>/var/log/dmesg</code>	<ul style="list-style-type: none">• This directory contains kernel ring buffer messages.• Information related to hardware devices and their drivers is recorded here.• It is very important because, due to their low-level nature, logging systems such as syslog are not running when these events take place and are unavailable to the administrator in real-time.
<code>/var/log/kern.log</code>	<ul style="list-style-type: none">• This file contains information logged by the kernel.
<code>/var/log/cron</code>	<ul style="list-style-type: none">• Cron is a service used to schedule automated tasks in Linux and this directory stores its events.• Whenever a scheduled task (or cron job) runs, all its relevant information including execution status and error messages are stored here.
<code>/var/log/mysqld.log</code> or <code>/var/log/mysql.log</code>	<ul style="list-style-type: none">• This is the MySQL log file.• All debug, failure and success messages related to the mysqld process and mysqld_safe daemon are logged here.

Monitoring Service Logs (Contd.)

- The command output shows a portion of /var/log/messages log file.
- Each line represents a logged event.
- The timestamps at the beginning of the lines mark the moment the event took place.

```
[analyst@secOps ~]$ sudo cat /var/log/messages
Mar 20 15:28:45 secOps kernel: Linux version 4.15.10-1-ARCH (builduser@heftig-18961) (gcc version 7.3.1
20180312 (GCC)) #1 SMP PREEMPT Thu Mar 15 12:24:34 UTC 2018
Mar 20 15:28:45 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-
4ddf-bfd8-c169e8a877b2 rw quiet
Mar 20 15:28:45 secOps kernel: KERNEL supported cpus:
Mar 20 15:28:45 secOps kernel: Intel GenuineIntel
Mar 20 15:28:45 secOps kernel: AMD AuthenticAMD
Mar 20 15:28:45 secOps kernel: Centaur CentaurHauls
Mar 20 15:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Mar 20 15:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Mar 20 15:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Mar 20 15:28:45 secOps kernel: x86/fpu: xstate_offset[2]: 576, xstate_sizes[2]: 256
Mar 20 15:28:45 secOps kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using
'standard' format.
Mar 20 15:28:45 secOps kernel: e820: BIOS-provided physical RAM map:
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x0000000001000000-0x0000000003ffff] usable
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x0000000003ffff0000-0x0000000003ffffff] ACPI data
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x00000000ffff0000-0x00000000ffffff] reserved
Mar 20 15:28:45 secOps kernel: NX (Execute Disable) protection: active
Mar 20 15:28:45 secOps kernel: random: fast init done
Mar 20 15:28:45 secOps kernel: SMBIOS 2.5 present.
Mar 20 15:28:45 secOps kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Mar 20 15:28:45 secOps kernel: Hypervisor detected: KVM
Mar 20 15:28:45 secOps kernel: e820: last_pfn = 0x3ffff0 max_arch_pfn = 0x40000000
Mar 20 15:28:45 secOps kernel: MTRR: Disabled
Mar 20 15:28:45 secOps kernel: x86/PAT: MTRRs disabled, skipping PAT initialization too.
Mar 20 15:28:45 secOps kernel: CPU MTRRs all blank - virtualized system.
```

Lab – Locating Log Files

- In this lab, you will get familiar with locating and manipulating Linux log files.

4.5 The Linux File System

The File System Types in Linux

- There are many different kinds of file systems, varying in properties of speed, flexibility, security, size, structure, logic and more.
- The administrator decides the file system type which is suitable for the operating system.
- The following table lists a few file system types commonly found and supported by Linux.

Linux File System	Description
ext2 (second extended file system)	<ul style="list-style-type: none">• ext2 was the default file system in several major Linux distributions until supplanted by ext3.• ext2 is still the file system of choice for flash-based storage media, as its lack of a journal, increases performance and minimizes the number of writes.• As flash memory devices have a limited number of write operations, minimizing write operations increases the device's lifetime.

The File System Types in Linux (Contd.)

Linux File System	Description
ext3 (third extended file system)	<ul style="list-style-type: none">• ext3 is a journaled file system designed to improve the existing ext2 file system.• A journal or log, the main feature added to ext3, is a technique used to minimize the risk of file system corruption in the event of sudden power loss.• The file systems keeps a log of all the changes to be made.• If the computer crashes before the change is complete, the journal can be used to restore or correct any issues created by the crash.• The maximum file size in ext3 file systems is 32 TB.
ext4 (fourth extended file system)	<ul style="list-style-type: none">• ext4 was created based on a series of extensions to ext3.• While the extensions improve the performance of ext3 and increase supported file sizes, developers were concerned about stability issues and were opposed to adding the extensions to the stable ext3.• The ext3 project was split in two; one kept as ext3 and its normal development and the other, named ext4, incorporated the mentioned extensions.

The File System Types in Linux (Contd.)

Linux File System	Description
NFS (Network File System)	<ul style="list-style-type: none">• NFS is a network-based file system, allowing file access over the network.• From the user standpoint, there is no difference between accessing a file stored locally or on another computer on the network.• NFS is an open standard which allows anyone to implement it.
CDFS (Compact Disc File System)	<ul style="list-style-type: none">• CDFS was created specifically for optical disk media.
Swap File System	<ul style="list-style-type: none">• The swap file system is used by Linux when it runs out of RAM.• When this happens, the kernel moves inactive RAM content to the swap partition on the disk.• While swap partitions can be useful to Linux computers with a limited amount of memory, they should not be considered as a primary solution.• Swap partition is stored on disk which has much lower access speeds than RAM.

The File System Types in Linux (Contd.)

Linux File System	Description
HFS Plus or HFS+ (Hierarchical File System Plus)	<ul style="list-style-type: none">• A file system used by Apple in its Macintosh computers.• The Linux kernel includes a module for mounting HFS+ for read-write operations.
APFS (Apple File System)	<ul style="list-style-type: none">• An updated file system that is used by Apple devices.• It provides strong encryption and is optimized for flash and solid-state drives.
Master Boot Record (MBR)	<ul style="list-style-type: none">• Located in the first sector of a partitioned computer, the MBR stores all the information about the way in which the file system is organized.• The MBR quickly hands over control to a loading function, which loads the OS.

The File System Types in Linux (Contd.)

- Mounting is the term used for the process of assigning a directory to a partition.
- After a successful mount operation, the file system contained on the partition is accessible through the specified directory.
- The command output shows the output of the mount command issued in the Cisco CyberOPS VM.

```
[analyst@secops ~]$ mount
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
sys on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
dev on /dev type devtmpfs (rw,nosuid,relatime,size=494944k,nr_inodes=123736,mode=755)
run on /run type tmpfs (rw,nosuid,nodev,relatime,mode=755)
/dev/sda1 on / type ext4 (rw,relatime)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
cgroup2 on /sys/fs/cgroup/unified type cgroup2 (rw,nosuid,nodev,noexec,relatime,nsdelegate)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,name=systemd)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
none on /sys/fs/bpf type bpf (rw,nosuid,nodev,noexec,relatime,mode=700)
cgroup on /sys/fs/cgroup/rdma type cgroup (rw,nosuid,nodev,noexec,relatime,rdma)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpu,cpuacct)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/hugetlb type cgroup (rw,nosuid,nodev,noexec,relatime,hugetlb)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup (rw,nosuid,nodev,noexec,relatime,net_cls,net_prio)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs
(rw,relatime,fd=29,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=11792)
debugfs on /sys/kernel/debug type debugfs (rw,nosuid,nodev,noexec,relatime)
tracefs on /sys/kernel/tracing type tracefs (rw,nosuid,nodev,noexec,relatime)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime,pagesize=2M)
mqueue on /dev/mqueue type mqueue (rw,nosuid,nodev,noexec,relatime)
tmpfs on /tmp type tmpfs (rw,nosuid,nodev)
```

Linux Roles and File Permissions

- Linux uses file permissions in order to organize the system and enforce boundaries within the computer.
- Every file in Linux carries its file permissions, which define the actions that the owner, the group, and others can perform with the file.
- The possible permission rights are Read, Write, and Execute.
- The ls command with the -l parameter lists additional information about the file.

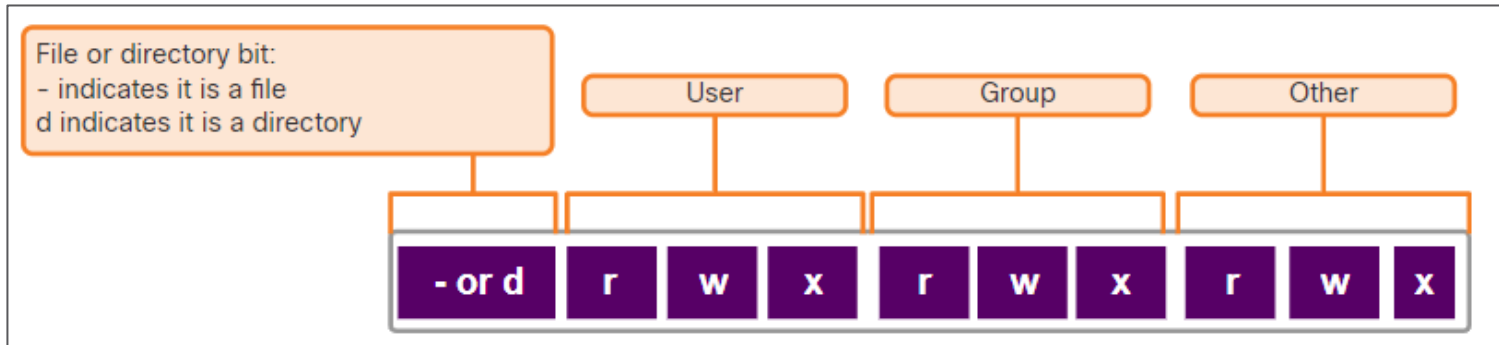
Linux Roles and File Permissions (Contd.)

- The output of the `ls -l` command provides a lot of information about the file `space.txt`:
 - The first field displays the permissions with `space.txt (-rwxrw-r--)`.
 - The second field defines the number of hard links to the file (number `1` after the permissions).
 - The third and fourth field display the user (`analyst`) and group (`staff`) who own the file, respectively.
 - The fifth field displays the file size in bytes. The `space.txt` file has 253 bytes.
 - The sixth field displays the date and time of the last modification.
 - The seventh field displays the file name.

```
[analyst@secOps ~]$ ls -l space.txt
-rwxrw-r-- 1 analyst staff 253 May 20 12:49 space.txt
(1)(2)(3)(4)(5)(6)(7)
[analyst@secOps ~]$
```

Linux Roles and File Permissions (Contd.)

- The figure here shows a breakdown of file permissions in Linux. The file **space.txt** has the following permissions:
- The dash (-) means that this is a file.
- The first set of characters (rwx) is for user permission. The user (analyst) who owns the file can Read, Write and eXecute the file.
- The second set of characters is for group permissions (rw-). The group (staff) who owns the file can Read and Write to the file.
- The third set of characters is for any other user or group permissions (r--) who can only Read the file.



Linux Roles and File Permissions (Contd.)

- Octal values are used to define permissions.
- File permissions are a fundamental part of Linux and cannot be broken.
- The only user that can override file permission on a Linux computer is the root user.

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

- A hard link is another file that points to the same location as the original file.
- Use the command `ln` to create a hard link.
- The first argument is the existing file and the second argument is the new file.
- As shown in the command output, the file `space.txt` is linked to `space.hard.txt` and the link field now shows 2.
- Both files point to the same location in the file system. If you change one file, the other is changed, as well.
- The `echo` command is used to add some text to `space.txt`.

```
[analyst@secOps ~]$ ln space.txt space.hard.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ ls -l space*
-rw-r--r-- 2 analyst analyst 239 May  7 18:18 space.hard.txt
-rw-r--r-- 2 analyst analyst 239 May  7 18:18 space.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ echo "Testing hard link" >> space.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ ls -l space*
-rw-r--r-- 2 analyst analyst 257 May  7 18:19 space.hard.txt
-rw-r--r-- 2 analyst analyst 257 May  7 18:19 space.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ rm space.hard.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ more space.txt
Space... The final frontier...
These are the voyages of the Starship Enterprise. Its continuing mission:
- To explore strange new worlds...
- To seek out new life; new civilizations...
- To boldly go where no one has gone before!
Testing hard link
[analyst@secOps ~]$
```

Hard Links and Symbolic Links (Contd.)

- A symbolic link, also called a symlink or soft link, is similar to a hard link in that applying changes to the symbolic link will also change the original file.
- As shown in the command output, use the ln command option -s to create a symbolic link.
- Notice that adding a line of text to test.txt also adds the line to mytest.txt.

```
[analyst@secOps ~]$ echo "Hello World!" > test.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ ln -s test.txt mytest.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ echo "It's a lovely day!" >> mytest.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ more test.txt
Hello World!
It's a lovely day!
[analyst@secOps ~]$
[analyst@secOps ~]$ rm test.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ more mytest.txt
more: stat of mytest.txt failed: No such file or directory
[analyst@secOps ~]$
[analyst@secOps ~]$ ls -l mytest.txt
lrwxrwxrwx 1 analyst analyst 8 May  7 20:17 mytest.txt -> test.txt
[analyst@secOps ~]$
```


Hard Links and Symbolic Links (Contd.)

- The following table shows several benefits of symbolic links over hard links:

Hard Links	Soft Links
Locating hard links is difficult.	Symbolic links show the location of the original file in the <code>ls -l</code> command.
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 as the system itself uses hard links to define the hierarchy of the directory structure.	Symbolic links can link to directories.

Lab - Navigating the Linux Filesystem and Permission Settings

- In this lab, you will familiarize yourself with Linux filesystems.

4.6 Working with the Linux GUI

X Window System

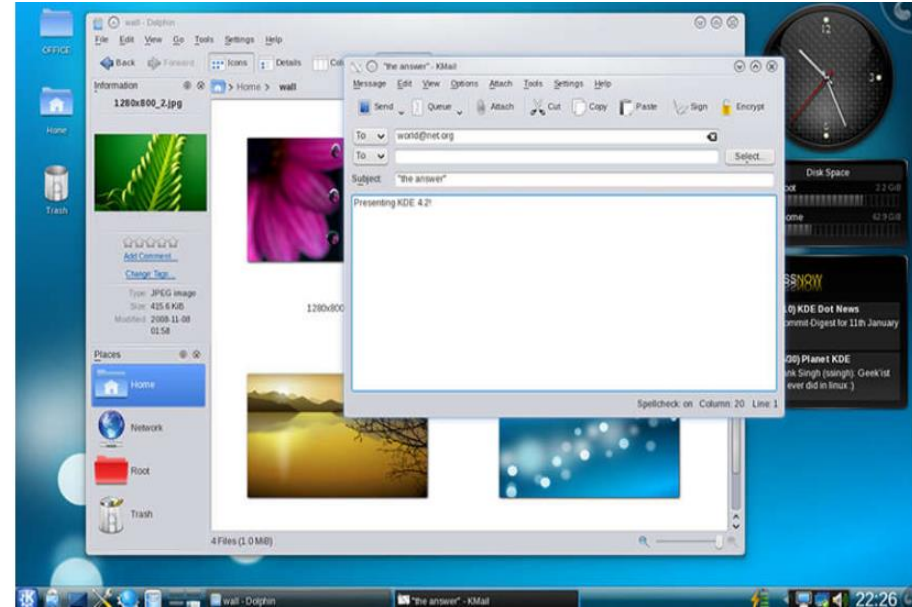
- The graphical interface present in most Linux computers is based on the X Window System.
- X Window, also known as X or X11, is a windowing system designed to provide the basic framework for a GUI.
- X includes functions for drawing and moving windows on the display device and interacting with a mouse and keyboard.
- X works as a server, which allows a remote user to use the network to connect, start a graphical application, and have the graphical window open on the remote terminal.
- X does not specify the user interface, leaving it to other programs, such as window managers, to define all the graphical components.

X Window System (Contd.)

- Examples of window managers are Gnome and KDE.



- The Gnome Window Manager



- The KDE Window Manager

4.7 Working on a Linux Host

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 libxen-4.6 libxenstore3.0 linux-libc-dev logrotate
openssh-client
qemu-block-extra qerau-kvm qemu-system-common qemu-system-x86 qemu-utils
```

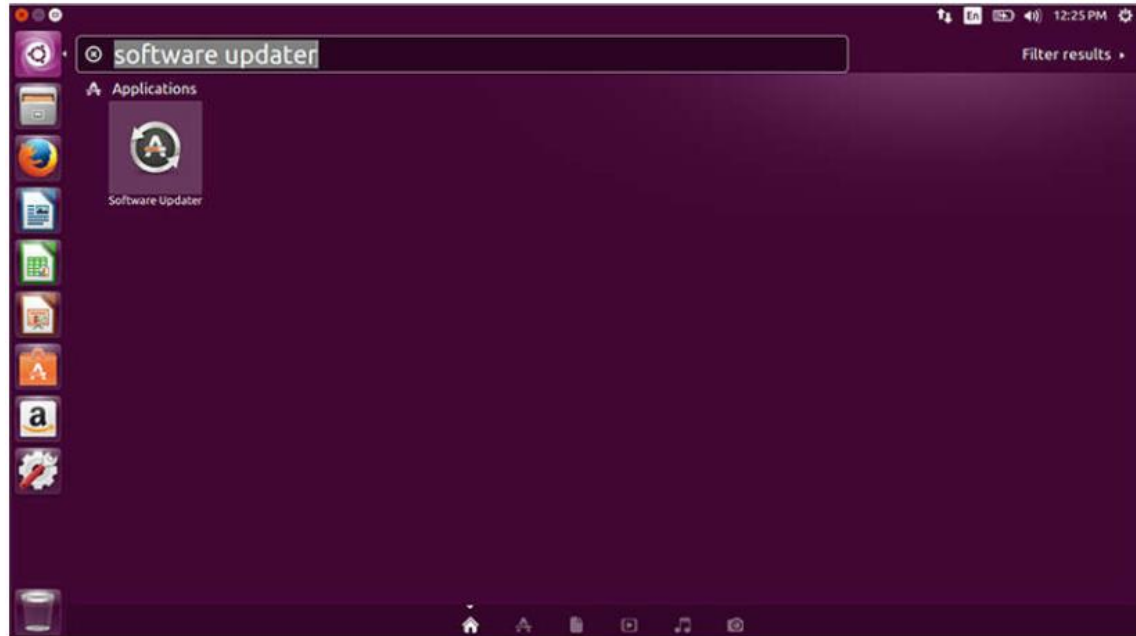
Keeping the System Up to Date

- 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	<code>pacman -S</code>	<code>apt install</code>
Remove a package by name	<code>pacman -Rs</code>	<code>apt remove</code>
Update a local package	<code>pacman -Syy</code>	<code>apt-get update</code>
Upgrade all currently installed packages	<code>pacman -Syu</code>	<code>apt-get upgrade</code>

Keeping the System Up to Date (Contd.)

- A Linux GUI can also be used to manually check and install updates.
- In Ubuntu for example, to install updates you would click Dash Search Box, type software updater, and then click the Software Updater icon.



Processes and Forks

- A process is a running instance of a computer program.
- Forking is a method that the kernel uses to allow a process to create a copy of itself.
- Processes need a way to create new processes in multitasking operating systems. The fork operation is the only way of doing so in Linux.
- When a process calls a fork, the caller process becomes the parent process and the newly created process becomes its child.
- After the fork, the processes are, to some extent, independent processes. They have different process IDs but run the same program code.

Processes and Forks (Contd.)

- The following table lists three commands that are used to manage

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

Processes and Forks (Contd.)

- The command output shows the output of the top command on a Linux computer.

```
[analyst@secOps ~]$ top
top - 11:29:16 up 0 min, 1 user, load average: 1.09, 0.31, 0.11
Tasks: 119 total, 1 running, 118 sleeping, 0 stopped, 0 zombie
%Cpu(s):  5.4 us,  2.0 sy,  0.0 ni, 87.4 id,  2.7 wa,  1.4 hi,  1.0 si,  0.0 st
MiB Mem :   982.8 total,    67.9 free,   765.8 used,   149.1 buff/cache
MiB Swap:    0.0 total,    0.0 free,    0.0 used,   39.3 avail Mem

  PID USER      PR  NI  VIRT  RES  SHR S %CPU  %MEM    TIME+  COMMAND
  729 analyst   20   0 2652376 284472 61076 S   2.7  28.3   0:06.75 Web Cont+
  570 analyst   20   0 2691388 215728 62404 S   2.0  21.4   0:06.99 firefox
  357 root       20   0 267972  91960 18468 S   1.3   9.1   0:01.63 Xorg
  461 analyst   20   0 322208  21000  7480 S   1.3   2.1   0:00.67 xfce4-p+
  121 root       20   0      0      0      0 S   0.7   0.0   0:00.43 kswapd0
    1 root       20   0 174376   4196  1688 S   0.3   0.4   0:00.66 systemd
  294 root       20   0 245036  11876   868 S   0.3   1.2   0:00.34 python2+
  539 analyst   20   0 150824    660    0 S   0.3   0.1   0:00.02 VBoxCli+
  800 analyst   20   0 477768  18968  9800 S   0.3   1.9   0:00.30 xfce4-t+
    2 root       20   0      0      0      0 S   0.0   0.0   0:00.00 kthreadd
    3 root       0 -20      0      0      0 I   0.0   0.0   0:00.00 rcu_gp
    4 root       0 -20      0      0      0 I   0.0   0.0   0:00.00 rcu_par+
    5 root       20   0      0      0      0 I   0.0   0.0   0:00.00 kworker+
    6 root       0 -20      0      0      0 I   0.0   0.0   0:00.00 kworker+
    7 root       20   0      0      0      0 I   0.0   0.0   0:00.00 kworker+
    8 root       0 -20      0      0      0 I   0.0   0.0   0:00.00 mm_perc+
    9 root       20   0      0      0      0 S   0.0   0.0   0:00.02 ksoftir+

[analyst@secOps ~]$
```

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.
- A rootkit is destructive as it changes kernel code and its modules, changing the most fundamental operations of the OS itself.
- 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

- Although command line tools are usually designed to perform a specific, well-defined task, many commands can be combined to perform more complex tasks by a technique known as piping.
- Piping consists of chaining commands together, feeding the output of one command into the input of another.
- 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 ~]$
```

Video Demonstration - Applications, Rootkits, and Piping

- Watch the video to view a demonstration of installing and updating applications, checking for a rootkit, and using piping commands.



Thank you! Questions?



Vladimír Veselý

updated: 2024-02-11

<https://www.fit.vutbr.cz/research/groups/nes@fit>