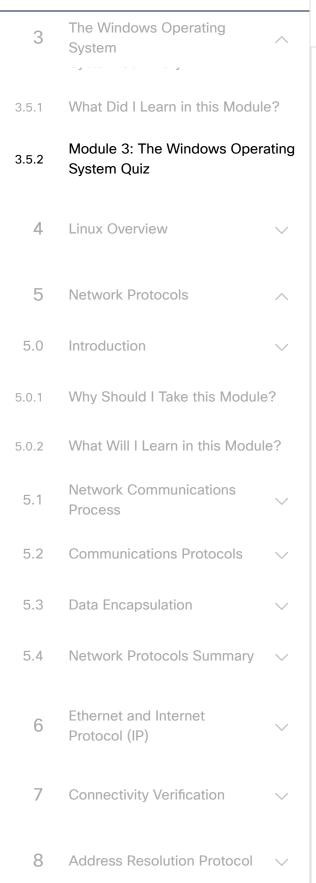
#### Show Menu



/ The Windows Operating System/ The Windows Operating System Summary

# The Windows Operating System Summary

3.5.1

### What Did I Learn in this Module?

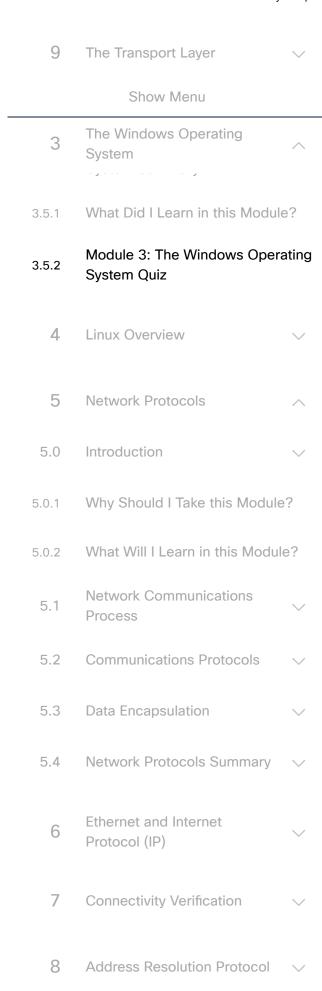


#### **Windows History**

The first computers required a Disk Operating System (DOS) to create and manage files. Microsoft developed MS-DOS as a command line interface (CLI) to access the disk drive and load the operating system files. Early versions of Windows consisted of a Graphical User Interface (GUI) that ran over MS-DOS. However, modern Windows versions are in direct control of the computer and its hardware and support multiple user processes. This is much different than the single process, single user MS-DOS. Since 1993, there have been more than 20 releases of Windows that are based on the NT operating system. Users use a Windows GUI to work with data files and software. The GUI has a main area that is known as the Desktop and a Task Bar situated below the desktop. The Task Bar includes the Start menu, quick launch icons, and a notification area. Windows has many vulnerabilities. Recommendations to secure the Windows OS include use of virus or malware protection, use of strong passwords, use of firewall, and limited use of the administrator account, among others.

#### **Windows Architecture and Operations**

Windows consists of a hardware abstraction layer (HAL) that is software that handles all of the communication



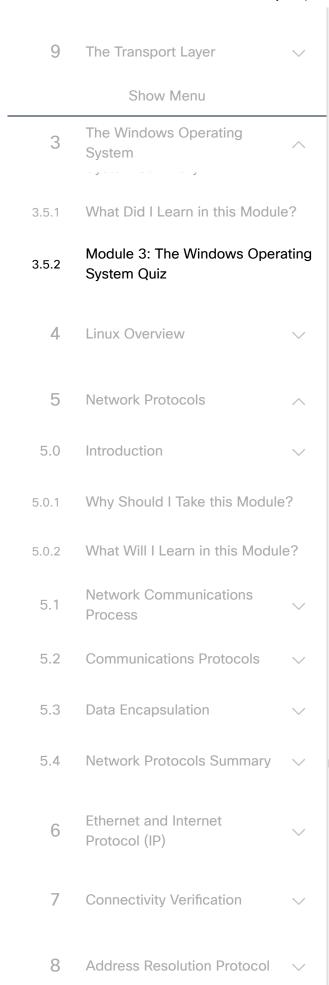
between the hardware and the kernel. The kernel has control over the entire computer and handles input and output requests, memory, and all of the peripherals connected to the computer. Windows operates in two different modes. The first is user mode. Most Windows programs run in user mode. The second is kernel mode. It allows operating system code direct access to the computer hardware. Windows supports several different file systems, but NTFS is the most widely used. NTFS volumes include the partition boot sector, master file table, system files and the file area. When a computer boots, it first accesses system information and code that is stored in BIOS hardware. The BIOS boot code performs a system self-test called POST, locates and loads the Windows OS, and loads other associated programs to start the operating system. Windows should always be shutdown properly.

A computer works by storing instructions in RAM until the CPU processes them. 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 up to 8 terabytes. Windows stores all of the information about hardware, applications, users, and system settings in a large database known as the registry. The registry is a hierarchical database where the highest level is known as a hive, below that there are keys, followed by subkeys. There are five registry hives that contain data regarding the configuration and operation of Windows. There are hundreds of keys and subkeys.

#### **Windows Configuration and Monitoring**

For security reasons, it is not advisable to log on to Windows using the Administrator account or an account with administrative privileges. Do not give standard users administrative privileges. Do not enable the Guests account unless the computer is going to be used by many different people who do not have accounts. Use Windows groups to make administration of users easier. Local users and groups are managed with the lusrmgr.msc control panel applet.

You can use the CLI or the Windows PowerShell to execute commands. PowerShell can be used to create scripts to automate tasks that the regular CLI is unable to automate. Windows Management Instrumentation (WMI) is used to manage remote computers. The **net** command



can be combined with switches to focus on specific output. Task Manager provides a lot of information about what is running, and the general performance of the computer. The Resource Monitor provides more detailed information about resource usage. The Network and Sharing Center is used to configure Windows networking properties and test networking settings. The Server Message Block (SMB) protocol is used to share network resources such as files on remote hosts. The Universal Naming Convention (UNC) format is used to connect to resources. Windows Server is an edition of Windows that is mainly used in data centers. It provides network, file, web, and management services to a Windows network or domain.

#### **Windows Security**

Malware can open communication ports to communicate and spread. The Windows netstat command displays all open communication ports on a computer and can also display the software processes that are associated with the ports. This enables unknown potentially malicious software to be identified and shutdown. Windows Event Viewer provides access to numerous logged events regarding the operation of a computer. Windows logs Windows events and applications and services events. Logged event severity levels range through the information, warning, error, or critical levels. It is very import to keep Windows up to date to guard against new security threats. Software patches, updates, and service packs address security vulnerabilities as they are discovered. Windows should be configured to automatically download and install updates as they become available. Windows can be configured to only install and restart a computer at specified times of day.

3.5.2

## Module 3: The Windows Operating System Quiz



9	The Transport Layer	~
	Show Menu	
3	The Windows Operating System	^
3.5.1	What Did I Learn in this Modul	e?
3.5.2	Module 3: The Windows Oper System Quiz	ating
4	Linux Overview	~
5	Network Protocols	^
5.0	Introduction	~
5.0.1	Why Should I Take this Module	e?
5.0.2	What Will I Learn in this Modul	le?
5.1	Network Communications Process	~
5.2	Communications Protocols	~
5.3	Data Encapsulation	~
5.4	Network Protocols Summary	~
6	Ethernet and Internet Protocol (IP)	~
7	Connectivity Verification	~
8	Address Resolution Protocol	<b>\</b>

1. When a user makes changes to the settings of a Windows system, where are these changes stored? ▼ Topic 3.2.0 - The registry contains information about applications, users, hardware, network settings, and file types.

The registry also contains a unique section for every user, which contains the settings

configured by that particular user.

- win.ini boot.ini Registry
- **Control Panel**
- 2. Which user account should be used only to perform system management and not as the account for regular use?
  - ✓ Topic 3.3.0 The administrator account is used to manage the computer and is very powerful. Best practices recommend that it be used only when it is needed to avoid accidentally performing significant changes to the system.
  - guest
  - administrator
  - power user
  - standard user

9	The Transport Layer	~
	Show Menu	
3	The Windows Operating System	^
3.5.1	What Did I Learn in this Modul	e?
3.5.2	Module 3: The Windows Open System Quiz	ating
4	Linux Overview	~
5	Network Protocols	^
5.0	Introduction	~
5.0.1	Why Should I Take this Module	e?
5.0.2	What Will I Learn in this Modul	e?
5.1	Network Communications Process	~
5.2	Communications Protocols	~
5.3	Data Encapsulation	<b>\</b>
5.4	Network Protocols Summary	~
6	Ethernet and Internet Protocol (IP)	~
7	Connectivity Verification	~
8	Address Resolution Protocol	~

- 3. Which command is used to manually query a DNS server to resolve a specific host name?
  - ✓ Topic 3.3.0 The **nslookup** command was created to allow a user to manually query a DNS server to resolve a given host name. The **ipconfig /displaydns** command only displays previously resolved DNS entries. The **tracert** command was created to examine the path that packets take as they cross a network and can resolve a hostname by automatically querying a DNS server. The **net** command is used to manage network computers, servers, printers, and network drives.

	nslookup
	tracert
	ipconfig /displaydns
	net
١.	For security reasons a network administrator needs
	to ensure that local computers cannot ping each
	other. Which settings can accomplish this task?

- Topic 3.4.0 Smartcard and file system settings do not affect network operation. MAC address settings and filtering may be used to control device network access but cannot be used to filter different data traffic types.
- smartcard settingsMAC address settingsfile system settingsfirewall settings
- 5. What contains information on how hard drive partitions are organized?

CPU	

			BOOTMGR
9	The Transport Layer	~	Windows Registry
	Show Menu		MBR
3	The Windows Operating System	^	6. What utility is used to show the system resources consumed by each user?
3.5.1	What Did I Learn in this Mo Module 3: The Windows O		
3.5.2	System Quiz		Event Viewer
4	Linux Overview	~	Device Manager User Accounts
5	Network Protocols	^	Task Manager
5.0	Introduction	~	7. What term is used to describe a logical drive that can be formatted to store data?
5.0.1	Why Should I Take this Mod	dule?	

### CyberOps Associate C

Process on the disk surface. Iracks are divided into sectors and multiple sectors are combined logically to form clusters 5.2 **Communications Protocols** track 5.3 Data Encapsulation sector cluster 5.4 **Network Protocols Summary** volume partition **Ethernet and Internet** 6 Protocol (IP) **Connectivity Verification** Address Resolution Protocol

9	The Transport Layer	~
	Show Menu	
3	The Windows Operating System	^
3.5.1	What Did I Learn in this Modul	e?
3.5.2	Module 3: The Windows Oper System Quiz	ating
4	Linux Overview	~
5	Network Protocols	^
5.0	Introduction	~
5.0.1	Why Should I Take this Module	e?
5.0.2	What Will I Learn in this Modul	e?
5.1	Network Communications Process	~
5.2	Communications Protocols	~
5.3	Data Encapsulation	~
5.4	Network Protocols Summary	~
6	Ethernet and Internet Protocol (IP)	~
7	Connectivity Verification	~
8	Address Resolution Protocol	<b>\</b>

8. How much RAM is addressable by a 32-bit version of Windows?
8 GB
○ 16 GB
32 GB
4 GB
9. Which Windows version was the first to introduce a 64-bit Windows operating system?
○ Windows NT
Windows XP
○ Windows 10
○ Windows 7

9	The Transport Layer	~
	Show Menu	
3	The Windows Operating System	^
3.5.1	What Did I Learn in this Modul	e?
3.5.2	Module 3: The Windows Oper System Quiz	ating
4	Linux Overview	~
5	Network Protocols	^
5.0	Introduction	~
5.0.1	Why Should I Take this Module	e?
5.0.2	What Will I Learn in this Modul	e?
5.1	Network Communications Process	~
5.2	Communications Protocols	~
5.3	Data Encapsulation	~
5.4	Network Protocols Summary	~
6	Ethernet and Internet Protocol (IP)	~
7	Connectivity Verification	~
8	Address Resolution Protocol	~

- 10. Which **net** command is used on a Windows PC to establish a connection to a shared directory on a remote server?

  - net accounts sets password and logon requirements for users
  - net session lists or disconnects sessions between a computer and other computers on the network
  - net share creates, removes, or manages shared resources
  - net start starts a network service or lists running network services
  - net stop stops a network service
  - net use connects, disconnects, and displays information about shared network resources
  - net view shows a list of computers and network devices on the network

	net share
	net use
	net start
	net session
11.	What is the purpose of the <b>cd</b> command?
	○ Topic 3.1.0 - CLI commands are typed into the Command Prompt window of the Windows operating system. The cd command is used to change the directory to the Windows root directory.
	changes directory to the previous directory
	changes directory to the next lower directory

changes directory to the next highest directory

changes directory to the root directory

9	The Transport Layer	~
	Show Menu	
3	The Windows Operating System	^
3.5.1	What Did I Learn in this Modul	e?
3.5.2	Module 3: The Windows Oper System Quiz	ating
4	Linux Overview	~
5	Network Protocols	^
5.0	Introduction	~
5.0.1	Why Should I Take this Module	e?
5.0.2	What Will I Learn in this Modul	e?
5.1	Network Communications Process	~
5.2	Communications Protocols	~
5.3	Data Encapsulation	~
5.4	Network Protocols Summary	~
6	Ethernet and Internet Protocol (IP)	~
7	Connectivity Verification	~
8	Address Resolution Protocol	~

- 12. What would be displayed if the **netstat abno** command was entered on a Windows PC?
  - Topic 3.4.0 With the optional switch abno, the netstat command will display all network connections together with associated running processes. It helps a user identify possible malware connections.
  - all active TCP and UDP connections, their current state, and their associated process ID (PID)
  - a local routing table
  - only active UDP connections in an LISTENING state
  - only active TCP connections in an ESTABLISHED state
- 13. A security incident has been filed and an employee believes that someone has been on the computer since the employee left last night. The employee states that the computer was turned off before the employee left for the evening. The computer is running slowly and applications are acting strangely. Which Microsoft Windows tool would be used by the security analyst to determine if and when someone logged on to the computer after working hours?
  - ⊙ Topic 3.4.0 Event Viewer is used to investigate the history of application, security, and system events. Events show the date and time that the event occurred along with the source of the event. If a cybersecurity analyst has the address of the Windows computer targeted or the date and time that a security breach occurred, the analyst could use Event Viewer to document and prove what occurred on the computer.
  - PowerShell
  - Performance Monitor
  - **Event Viewer**

