CCNA Cyber Ops (Version 1.1) – Chapter 2 Exam Answers Full

🆔 **itexamanswers.net**/ccna-cyber-ops-chapter-2-exam-answers-full.html

How to find: Press **"Ctrl + F"** in the browser and fill in whatever wording is in the question to find that question/answer. If the question is not here, find it in **Questions Bank**.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

1. What contains information on how hard drive partitions are organized?

- CPU
- **MBR**
- BOOTMGR
- Windows Registry

B. The master boot record (MBR) contains a small program that is responsible for locating and loading the operating system. The BIOS executes this code and the operating system starts to load.

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

- **net use**
- net start
- net share
- net session

A. The net command is a very important command in Windows. Some common net commands include the following:
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 resourcesnet 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

3. Which type of startup must be selected for a service that should run each time the computer is booted?

- Boot
- Manual
- **Automatic**
- Start
- Startup

C. An automatic startup will start the service automatically when the PC starts. The manual
startup process will occur when the application is launched by a user. There is no boot, start,
or startup service type that can be configured.

4. A user creates a file with a .ps1 extension in Windows. What type of file is it?

- PowerShell cmdlet
- PowerShell function
- PowerShell documentation
- **PowerShell script**

D. The types of commands that PowerShell can execute include the following:
Cmdlets: Perform an action and return an output or object to the next command that will be
executed
PowerShell scripts: Files with a .ps1 extension that contain PowerShell commands that are
executed
PowerShell functions: Pieces of code that can be referenced in a script

5. When a user makes changes to the settings of a Windows system, where are these changes stored?

- Control panel
- **Registry**
- win.ini
- boot.ini

B. 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.

6. Which Windows version was the first to introduce a 64-bit Windows operating system?

- Windows NT
- **Windows XP**
- Windows 7
- Windows 10

B. There are more than 20 releases and versions of the Windows operating system. The Windows XP release introduced 64-bit processing to Windows computing.

7. Two pings were issued from a host on a local network. The first ping was issued to the IP address of the default gateway of the host and it failed. The second ping was issued to the IP address of a host outside the local network and it was successful. What is a possible cause for the failed ping?

- The default gateway device is configured with the wrong IP address.
- The TCP/IP stack on the default gateway is not working properly.
- The default gateway is not operational.
- **Security rules are applied to the default gateway device, preventing it from processing ping requests.**

D. If the ping from one host to another host on a remote network is successful, this indicates that the default gateway is operational. In this scenario, if a ping from one host to the default gateway failed, it is possible that some security features are applied to the router interface, preventing it from responding to ping requests.

8. Which command is used to manually query a DNS server to resolve a specific hostname?

- net
- tracert
- **nslookup**
- ipconfig /displaydns

C. 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.

9. What is the purpose of the cd\ command?

- changes directory to the previous directory
- **changes directory to the root directory**
- changes directory to the next highest directory

- changes directory to the next lower directory

B. 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.

10. How much RAM is addressable by a 32-bit version of Windows?

- **4 GB**
- 8 GB
- 16 GB
- 32 GB

A. A 32-bit operating system is capable of supporting approximately 4 GB of memory. This is because 2^{32} is approximately 4 GB.

11. How can a user prevent specific applications from accessing a Windowscomputer over a network?

- Enable MAC address filtering.
- Disable automatic IP address assignment.
- **Block specific TCP or UDP ports in Windows Firewall.**
- Change default usernames and passwords.

C. Network applications have specific TCP or UDP ports that can be left open or blocked in Windows Firewall. Disabling automatic IP address assignment may result in the computer not being able to connect to the network at all. Enabling MAC address filtering is not possible in Windows and would only block specific network hosts, not applications. Changing default usernames and passwords will secure the computer from unauthorized users, not from applications.

12. What utility is used to show the system resources consumed by each user?

- **Task Manager**
- User Accounts
- Device Manager
- Event Viewe

A. The Windows Task Manager utility includes a Users tab from which the system resources consumed by each user can be displayed.

13. What utility is available on a Windows PC to view current running applications and processes?

- nslookup
- ipconfig

- Control Panel
- **Task Manager**

On a Windows PC the Task Manager utility can be used to view the applications, processes, and services that are currently running.

14. A user logs in to Windows with a regular user account and attempts to use an application that requires administrative privileges. What can the user do to successfully use the application?

- Right-click the application and choose Run as root.
- Right-click the application and choose Run as Priviledge.
- **Right-click the application and choose Run as Administrator.**
- Right-click the application and choose Run as Superuser.

As a security best practice, it is advisable not to log on to Windows using the Administrator account or an account with administrative privileges. When it is necessary to run or install software that requires the privileges of the Administrator, the user can right-click the software in the Windows File Explorer and choose Run as Administrator.

15. A technician can ping the IP address of the web server of a remote company but cannot successfully ping the URL address of the same web server. Which software utility can the technician use to diagnose the problem?

- **nslookup**
- tracert
- netstat
- ipconfig

Traceroute (tracert) is a utility that generates a list of hops that were successfully reached along the path from source to destination. This list can provide important verification and troubleshooting information. The ipconfig utility is used to display the IP configuration settings on a Windows PC. The Netstat utility is used to identify which active TCP connections are open and running on a networked host. Nslookup is a utility that allows the user to manually query the name servers to resolve a given host name. This utility can also be used to troubleshoot name resolution issues and to verify the current status of the name servers.

16. Where are the settings that are chosen during the installation process stored?

- in the recovery partition
- in flash memory
- **in the Registry**

- in BIOS

The Registry contains all settings chosen from Control Panels, file associations, system policies, applications installed, and application license keys.

17. What technology was created to replace the BIOS program on modern personal computer motherboards?

- CMOS
- MBR
- RAM
- **UEFI**

As of 2015, most personal computer motherboards are shipped with UEFI as the replacement for the BIOS program.

18. Which two things can be determined by using the *ping* command? (Choose two.)

- the number of routers between the source and destination device
- **the destination device is reachable through the network**
- the average time it takes each router in the path between source and destination to respond
- the IP address of the router nearest the destination device
- **the average time it takes a packet to reach the destination and for the response to return to the source**

A ping command provides feedback on the time between when an echo request was sent to a remote host and when the echo reply was received. This can be a measure of network performance. A successful ping also indicates that the destination host was reachable through the network.

19. What function is provided by the Windows Task Manager?

- It provides an active list of TCP connections.
- It maintains system logs.
- It selectively denies traffic on specified interfaces.
- **It provides information on system resources and processes.**

Windows Task Manager enables an end user to monitor applications, processes, and services currently running on the end device. It can be used to start or stop programs, stop processes, and display informative statistics about the device.

20. Which type of Windows PowerShell command performs an action and returns an output or object to the next command that will be executed?

- scripts
- functions
- **cmdlets**
- routines

The types of commands that PowerShell can execute include the following:cmdlets – perform an action and return an output or object to the next command that will be executed PowerShell scripts – files with a .ps1 extension that contain PowerShell commands that are executed
PowerShell functions – pieces of code that can be referenced in a script

21. What would be displayed if the *netstat -abno* command was entered on a Windows PC?

- **all active TCP and UDP connections, their current state, and their associated process ID (PID)**
- only active TCP connections in an ESTABLISHED state
- only active UDP connections in an LISTENING state
- a local routing table

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.

22. Which two commands could be used to check if DNS name resolution is working properly on a Windows PC? (Choose two.)

- ipconfig /flushdns
- net cisco.com
- **nslookup cisco.com**
- **ping cisco.com**
- nbtstat cisco.com

The ping command tests the connection between two hosts. When ping uses a host domain name to test the connection, the resolver on the PC will first perform the name resolution to query the DNS server for the IP address of the host. If the ping command is unable to resolve the domain name to an IP address, an error will result.

Nslookup is a tool for testing and troubleshooting DNS servers.

23. Refer to the exhibit. A cyber security administrator is attempting to view system information from the Windows PowerShell and recieves the error message shown. What action does the administrator need to take to successfully run the command?

```
PS C:\Users\CyberOpsUser> netstat -abno
The requested operation requires elevation.
PS C:\Users\CyberOpsUser> netstat -abno
```

- Run the command from the command prompt.
- Install latest Windows updates.
- Restart the abno service in Task Manager.
- **Run PowerShell as administrator.**

Best practices advise not to log into systems with an administrator account, but rather a user account. When logged in as a user it is possible to run Windows utilitites, such as PowerShell and the Command Prompt as an administrator by right clicking on the utility and slecting Run as Administrator.

24. Refer to the exhibit. A cybersecurity analyst is investigating a reported security incident on a Microsoft Windows computer. Which tool is the analyst using?
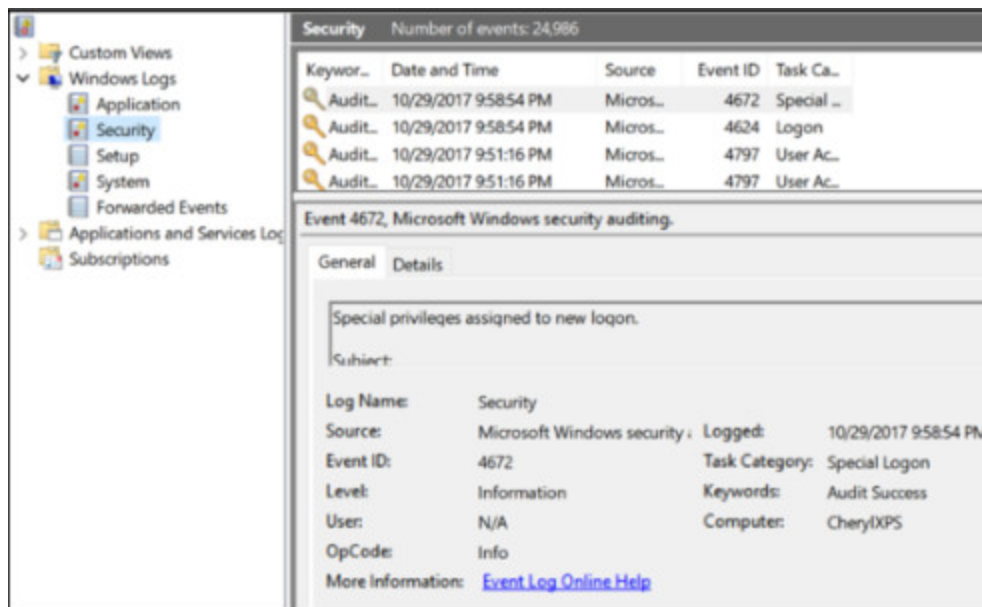
- **Event Viewer**
- PowerShell
- Task Manager
- Performance Monitor

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 and/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.

25. For security reasons a network administrator needs to ensure that local computers cannot ping each other. Which settings can accomplish this task?

- **firewall settings**
- MAC address settings
- smartcard settings
- file system settings

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.

26. Consider the path representation in Windows CLI C:\Users\Jason\Desktop\mydocu.txt. What does the Users\Jason component represent?

- **file directory and subdirectory**
- current file directory
- file attribute
- storage device or partition

In the path representation in Windows CLI, the components of C:\Users\Jason\Desktop\mydocu.txt are as follows:C:\ represents the root directory of the storage device.
Users\Jason represents the file directory.
Desktop represents the current file directory.
The mydocu.txt represents the user file.

27. Which two user accounts are automatically created when a user installs Windows to a new computer? (Choose two.)

- superuser
- **guest**
- root
- **administrator**
- system

When a user installs Windows, two local user accounts are created automatically during the process, administrator and guest.

28. What term is used to describe a logical drive that can be formatted to store data?

- **partition**
- track

- sector
- cluster
- volume

Hard disk drives are organized by several physical and logical structures. Partitions are logical portions of the disk that can be formatted to store data. Partitions consist of tracks, sectors, and clusters. Tracks are concentric rings on the disk surface. Tracks are divided into sectors and multiple sectors are combined logically to form clusters

29. What is the purpose of entering the *netsh* command on a Windows PC?

- to create user accounts
- to test the hardware devices on the PC
- to change the computer name for the PC
- **to configure networking parameters for the PC**

The netsh.exe tool can be used to configure networking parameters for the PC from a command prompt.

30. A technician is troubleshooting a PC unable to connect to the network. What command should be issued to check the IP address of the device?

- **ipconfig**
- ping
- tracert
- nslookup

The commands tracert and ping are used to test the connectivity of the PC to the network. The command nslookup initiates a query to an Internet domain name server.

31. Refer to the exhibit. Which Microsoft Windows application is being used?
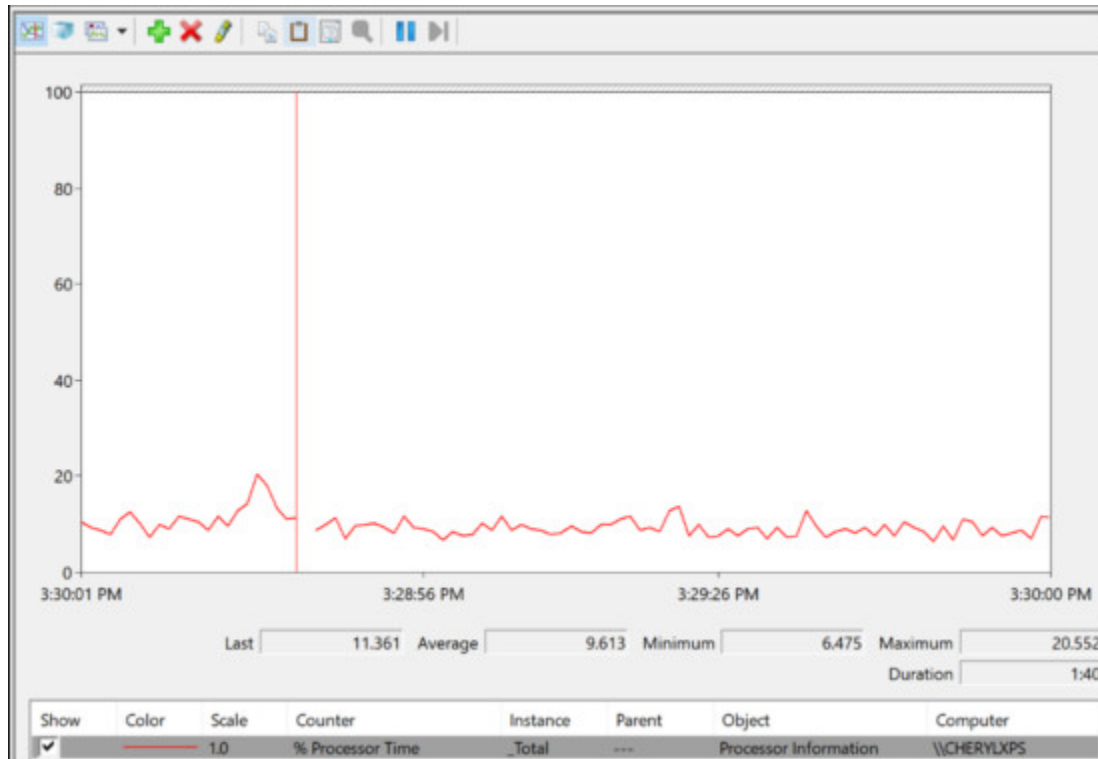
- Event Viewer
- PowerShell
- Task Manager
- **Performance Monitor**

Windows Performance Monitor is used to evaluate the performance of individual components on a Windows host computer. Commonly monitored components include the processor, hard drive, network, and memory. Windows Task Manager and Performance Monitor are used when malware is suspected and a component is not performing the way it should.

32. What are two reasons for entering the *ipconfig* command on a Windows PC? (Choose two.)

- **to review the network configuration on the PC**
- to check if the DNS server can be contacted
- to ensure that the PC can connect to remote networks
- **to review the status of network media connections**
- to display the bandwidth and throughput of the network connection

The command ipconfig is a useful tool for troubleshooting. The command will display some IP addressing configuration and the network media connection status. The command does not test the connection to the DNS server configured or test remote networks. It does not display bandwidth and throughput information.

33. What are two advantages of the NTFS file system compared with FAT32? (Choose two.)

- NTFS allows the automatic detection of bad sectors.
- NTFS is easier to configure.
- NTFS allows faster formatting of drives.
- **NTFS provides more security features.**
- **NTFS supports larger files.**
- NTFS allows faster access to external peripherals such as a USB drive.

The file system has no control over the speed of access or formatting of drives, and the ease of configuration is not file system-dependent.

34. What is the purpose of using the *net accounts* command in Windows?

- to start a network service
- to display information about shared network resources
- to show a list of computers and network devices on the network
- **to review the settings of password and logon requirements for users**

These are some common net commands:
net accounts – sets password and logon requirements for users
net start – starts a network service or lists running network services
net use – connects, disconnects, and displays information about shared network resources
net view – shows a list of computers and network devices on the network
When used without options, the net accounts command displays the current settings for password, logon limitations, and domain information.

35. What are two reasons for entering the *ping 127.0.0.1* command on a Windows PC? (Choose two.)

- **to check if the NIC functions as expected**
- to check if the default gateway is configured correctly
- to display the bandwidth and throughput of the network connection
- **to check if the TCP/IP protocol suite is installed properly**
- to ensure that the PC can connect to remote networks

The IP address 127.0.0.1 is a loopback address on the PC. A successful ping to the loopback address indicates that the TCP/IP protocol suite is installed properly and the NIC is working as expected. A ping to the loopback address does not test the connectivity to remote networks, nor will it display bandwidth and throughput information.
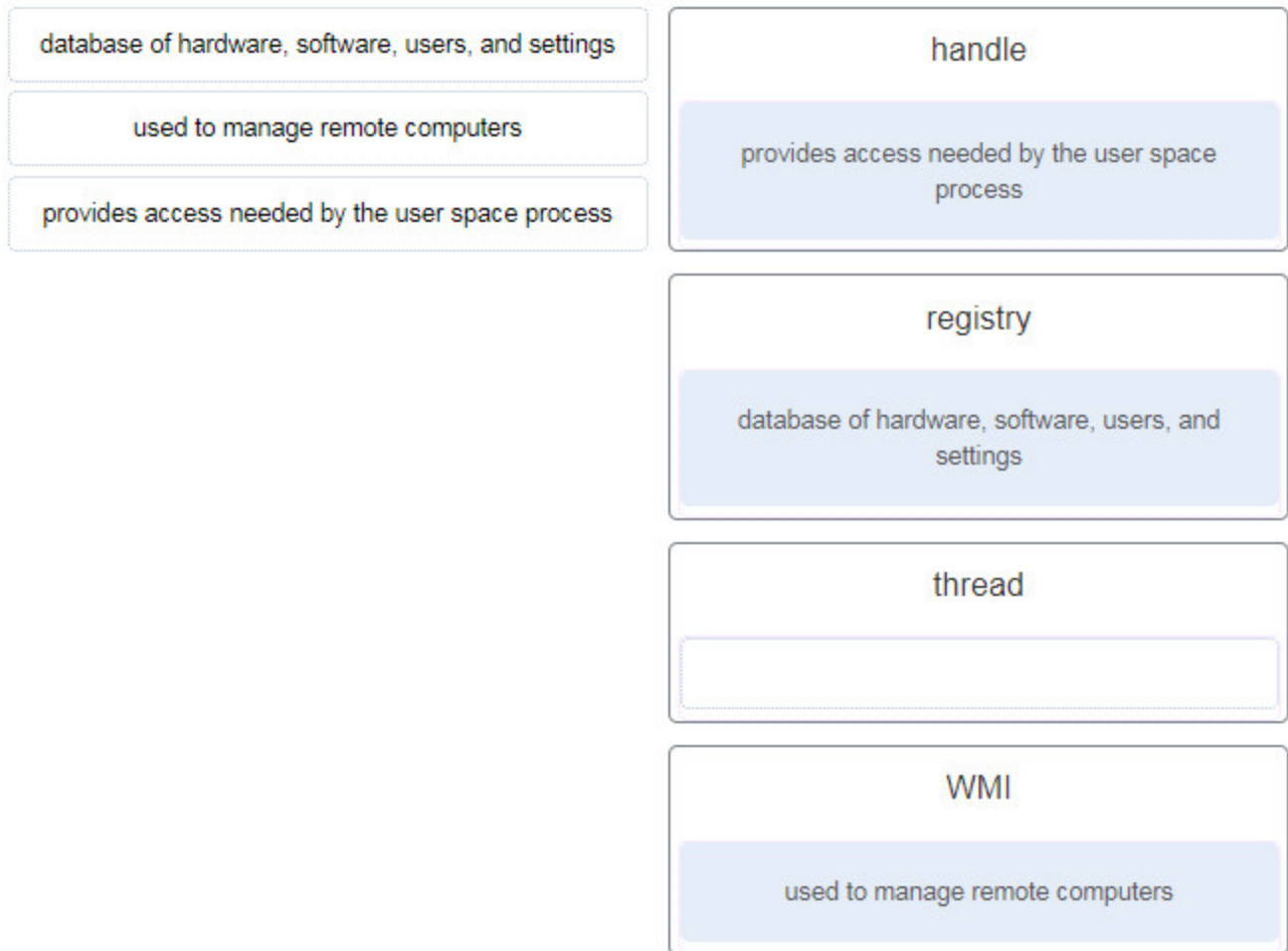
36. When restrictive security policy is implemented on a firewall, only certain required ports are opened

37. Match the Windows command to the description.

| Commands	Descriptions
dir	renames a file
mkdir	**ren**
cd	creates a new directory
ren	**mkdir**
	changes the current directory
	cd
	lists files in a directory
	dir

- dir ~~> lists files in a directory
- mkdir ~~> creates a new directory
- cd ~~> changes the current directory
- ren ~~> renames a file

38. Match the definition to the Microsoft Windows term. (Not all options are used.)

|	
database of hardware, software, users, and settings	**handle** provides access needed by the user space process
used to manage remote computers	**registry** database of hardware, software, users, and settings
provides access needed by the user space process	**thread**
	WMI used to manage remote computers

- runs in the background to support the operating system and applications ~~> service
- instructions executed by the processor ~~> thread
- a currently executing program ~~> process
- (empty) ~~> registry

39. Match the definition to the Microsoft Windows term. (Not all options are used.)

runs in the background to support the operating system and applications	**process**
	a currently executing program
instructions executed by the processor	
	registry
a currently executing program	
	service
	runs in the background to support the operating system and applications
	thread
	instructions executed by the processor
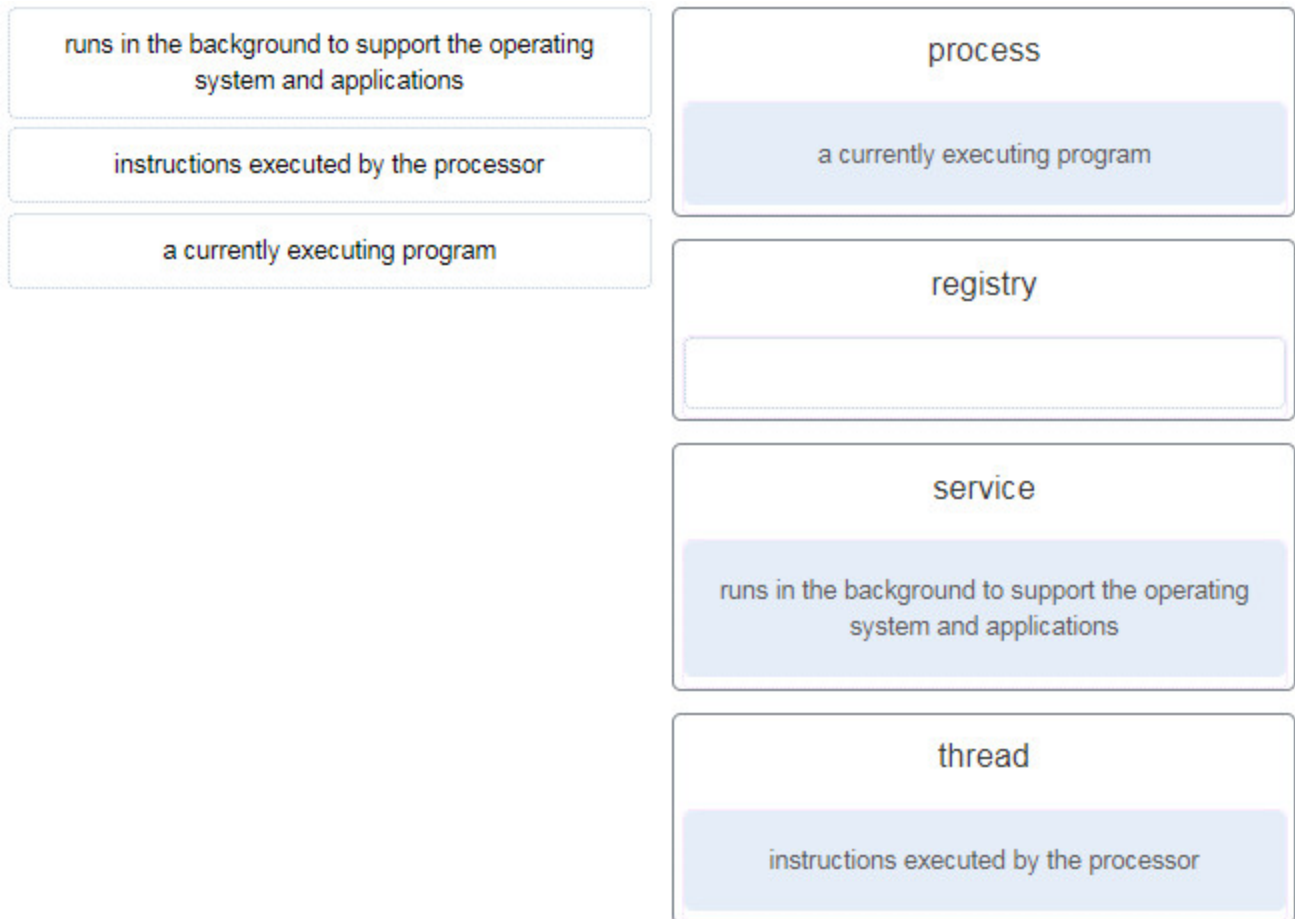
- database of hardware, software, users, and settings ~~> registry
- used to manage remote computers ~~> WMI
- provides access needed by the user space process ~~> handle
- (empty) ~~> thread

40. Match the Windows term to the description.
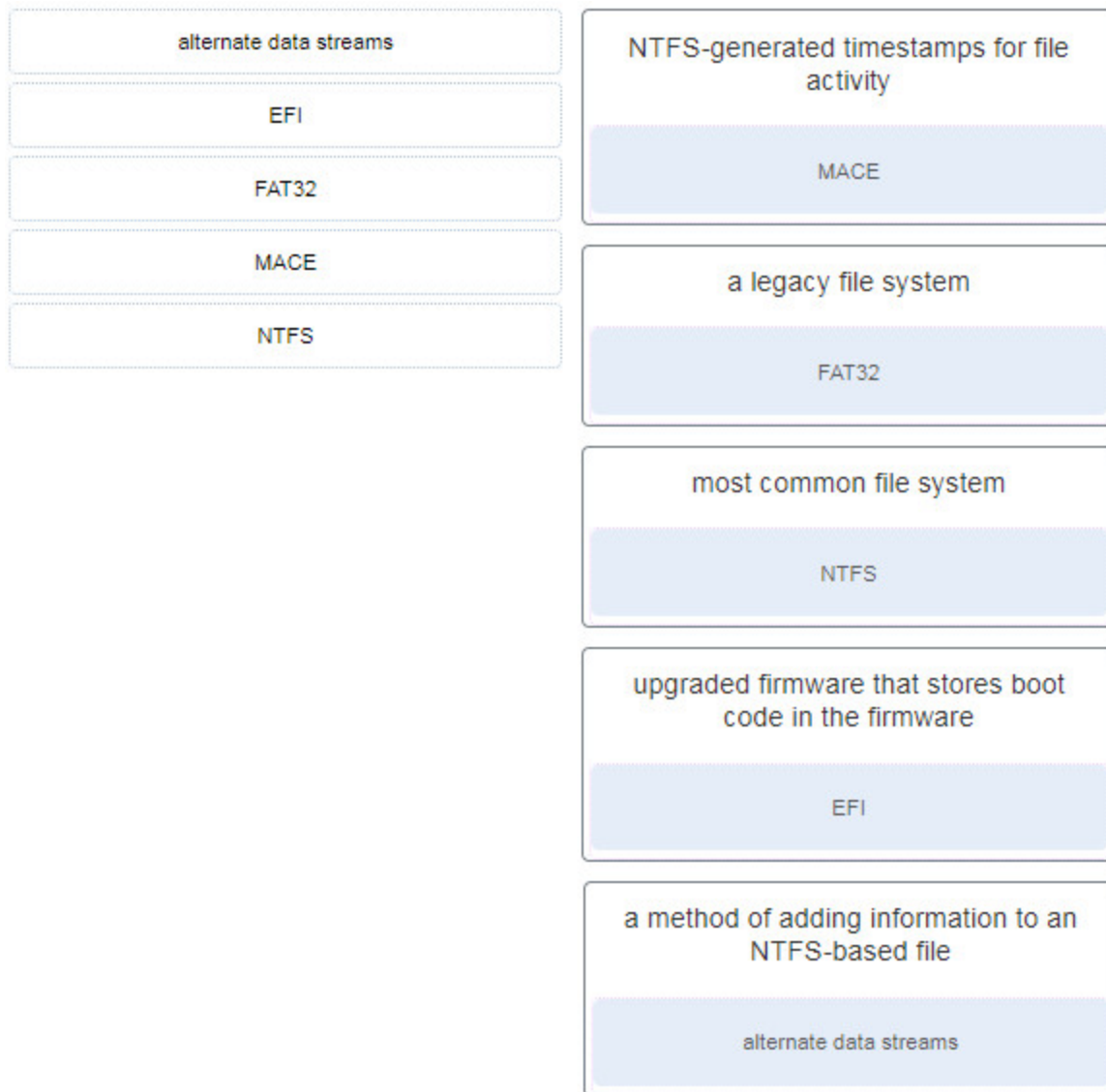
- alternate data streams ~~> a method of adding information to an NTFS-based file
- EFI ~~> upgraded firmware that stores boot code in the firmware
- FAT32 ~~> a legacy file system
- MACE ~~> NTFS-generated timestamps for file activity
- NTFS ~~> most common file system

Download PDF File below:

[sociallocker id="54558"]

CCNA Cybersecurity Operations (Version 1.1) - CyberOps Chapter 2 Exam Answers.pdf   428.56 KB   1574 downloads

...

[/sociallocker]