**Windows commands:**

DISM windows command

SFC windows command

Tasklist

Taskkill /IM <process name>

Taskkill /PID <task process ID> /t

Gpupdate

The difference between copy, xcopy and robocopy

Xcopy copies file permissions

Services.msc or net start/stop command

Chkdsk /f and /r

**Windows Certification:**

Research these windows tools:

Memory diagnostics

Component services

Odbc data sources

**Hardware:**

**Physical Address Extension (PAE)** enables 32 bit OS to utilize more than 4GB of memory

PAE only allows you to use up to 64gb of memory, not the 16 exabytes in 64 bit architecture

**Windows 8 and later requires CPUs to be capable of PAE**

The processor must be running in Physical Address Extension (PAE) mode to use the **NX bit** processor feature. The NX bit is a form of memory protection that provides additional security.

Intel: **XD bit (*execute disable*)**, AMD: **Enhanced Virus Protection** (**EVP**)

**SSE2** refers to a solution (a complimentary instruction set) that extends the capabilities of a CPU. All processors that support NX also support SSE2

SSE data transfers use XMM register

File attributes:

Read Only

Archive

System

Hidden

Windows extended attributes

Index

Compression

encryption

Attrib windows command

Relative path vs direct path

Partitioning schemes:

MBR for PC BIOS-based systems

GPT for UEFI-based systems

MBR:

Four primary partitions, 3 primary and 1 extended

One marked active

2tb partition size limit

All primaries contain data

Boot sectors become populated on active partitions called system partitions

Boot partition is where the operating system resides

GPT:

Newer partitioning

Allows for 128 partitions

Backwards compatible with BIOS-based systems

Boot code redundancy

No 2TB partition size limit

List disk

An asterisk means its GPT, no asterisk means its MBR

The theoretical memory limits in 16, 32 and 64 bit machines are as follows:

16 bit = 65, 536 bytes (64 Kilobytes)

32 bit = 4, 294, 967, 295 bytes (4 Gigabytes)

64 bit = 18, 446, 744, 073, 709, 551, 616 (16 Exabytes)

x86 is 32bit architecture

NTFS and ACL

What does the USMT tool do?: Migrates user setting and files from one OS to another

You use a class B fire extinguisher to put out electrical fires

What are the different classes of fire extinguishers?

**Steps to remove any malware:**

1. Identify and research malware symptoms
2. Quarantine infected systems
3. Disable system restore (Windows)
4. Remediate the infected system
5. Update (or install) anti-malware software
6. Scan and use removal techniques (safe mode, pre-installation environment)
7. Schedule scans and run updates
8. Enable system restore and create a restore point (Windows)
9. Educate the end user

You use the bcdedit.exe utility to edit, modify and update the boot configuration data (BCD) file, which contains boot settings for a computer. You could also change the boot order by using the MSCONFIG tool

If you want your computer to boot faster and access more RAM at startup, disable application startup.

Wearing leather soled shoes will help transfer electricity. Some rubber soled trues protect against ESD if the soles are made up of conductive rubber that scatters static electricity

What is Windows 8 RT?

All versions of Windows after Windows 8 support MUI (multilingual user interface)

So does Windows 7 Ultimate

MSDS, OSHA and EPA guidelines

Single-Sign-On (SSO) ensures that users are able to log in to multiple system using the same login credentials

Windows 7 allows you to boot the computer into Windows XP mode on a computer that supports virtualization.

Attributes of a person that can be used to grant biometric access:  
Fingerprints, face, signature, iris, retina, hand geometry, voice

Windows 7 can be upgraded to Windows 8 basic or pro

The task scheduler tool can be used to periodically create a Restore Point

Spotlight in mac: command + spacebar

What is the dock (mac)

Redhat, fedora, centos: yum update

Most of the other distros follow debian model: apt (apt-get) update

Apt dist-upgrade

DD command

Automated System Recovery is not an option listed in the Advanced Boot Options menu

If you get the following error the registry is corrupt:

Windows 8.1 could not start because the following file is missing or corrupt: \WINDOWS\SYSTEM32\CONFIG\SYSTEM

You are putting your registry file in jeopardy when you shut down your computer improperly

BranchCache helps reduce repetitive traffic over a WWAN

R sync

Mac OS X troubleshooting:

Physical security

Entry access control roster.

Man traps

Security guards

Access cards with RFID chips

Magnet locks unlock when power goes out

Desk mount (laptop lock)

Smart cards, CAT cards

Software token and hardware tokens

RSA secure ID key fob

Like the google or blizz authenticator

User security vs data security

User authentication and authorization

Password policies

Something you know, something you are, something you have authentication

Examples of something you have authentication:

Door locks, server locks and hardware tokens

MDM mobile device management

Data loss prevention (DLP)

Principle of least privilege

Access control lists

When a policy change is made in active directory, the policy is applied at logon

What are active directory policies?

What is folder redirection?

What is a logical domain (security boundary)?

FAT32 doesn’t allow ACL and permissions

Perfmon and resmon

Effective access lists lets you find troubleshoot file and folder access issues

When you have conflicting permissions on a user or a file, the most restrictive permission will always win out

If you have BIOS, you need two NTFS partitions

If you have UEFI, you need one FAT32 and an NTFS partition

A virus relies on other applications to execute and infect the system

EFS vs bitlocker

Bitlocker can be used in non TPM mode, but lowers security

It will use a USB key instead of a set of bits on the motherboard

Microsoft azure: microsoft intune, device compliance

Radius and TACACS servers. Radius does not provide accounting (what did the user do when he logged in) but is just as good as TACACS at authentication and authorization

When you’re infected with a virus, disable system restore.

**BranchCache:** allows computers at a local branch office to cache data from a file or web server on a WAN (wide area network)

**The difference between EFS and Bitlocker/TPM:** EFS allows you to encrypt certain sectors of the hard drive while TPM can be used to encrypt the entire hard drive. Windows home versions do not have TPM, TPM is needed to use Bitlocker.

**MSTSC shell command:** Creates connections to Remote Desktop Session Host servers or other remote computers, edits an existing Remote Desktop Connection (.rdp) configuration file, and migrates legacy connection files that were created with Client Connection Manager to new .rdp connection files.

**.vbs files** are virtual basic scripts. Most scripting is done through powershell now. .vbs scripts are also used in Microsoft Excel

**SSE2** (**Streaming SIMD Extensions 2**) is one of the Intel SIMD (Single Instruction, Multiple Data) processor supplementary instruction sets first introduced by Intel with the initial version of the Pentium 4 in 2000. It extends the earlier SSE instruction set, and is intended to fully replace MMX.

**MSI files** are used for installation, storage, and removal of programs in Windows

**MMC** is the windows GUI shell for administrative and even some non-administrative snap-ins

**Certmgr.msc** is an MMC snap-in

Short for Resource Monitor, **Resmon** is a feature introduced with Windows Vista that enables users to view real-time resource information about software and hardware on their computer. It shows things like memory, disk, CPU and network performance, as well as which software handles and file modules are working

**PERFMON** is a Caché utility that controls the MONITOR facility. The MONITOR facility provides performance data for the Caché system by collecting counts of events at the system level and sorting the metrics by process, routine, global, and network nodes.

**Chkdsk:** verifies the file system integrity of a volume and fixes logical file system errors

**Disk Clean-up:** is a computer maintenance utility included in Microsoft Windows designed to free up disk space on a computer's hard drive. The utility first searches and analyzes the hard drive for files that are no longer of any use, and then removes the unnecessary files...The

**Windows Event Viewer** shows a log of application and system messages, including errors, information messages, and warnings. It’s a useful tool for troubleshooting all kinds of different Windows problems.

**CDFS (compact disk file system)** is a file system for read-only and write-once CD-ROMs.

**Universal Disk Format:** has been most widely used for DVDs and newer optical disc formats, supplanting ISO 9660/CDFS

**FAT32** has a 4hb max file size and a 32gb max hard drive size

**NTFS:** most popular windows file system. Insanely huge file size limits so in practice, no maximum file size. Also allows file permissions and encryption. Windows must be installed on an NTFS formatted partition. NTFS is read only in MacOS and older linux distros.

**exFAT:** designed as an upgrade from FAT, used mostly in memory cards (SD). has wider non-windows support

**ext2, ext3, ext4:** extended file system developer for linux

**HFS, HFS+, APFS:** apple file system

You use a different file system depending on your OS:

* NTFS for Windows
* HFS+/APFS for MacOS
* ext4 for linux

Use FAT32 on removable media below 32 gbs and exFAT on anything bigger

You can use as many disks as you want with a striped volume

A mirrored volume uses a maximum of 2 disks

You need to enable wake on LAN. where would you go to do this?

Firewalls are port security?

Certificates

Press F8 on boot in Windows 7 to enable System Recovery

The NTLDR was replaced by the boot.ini file

Mutual or two-way authentication checks the identity of both ends of the connection

What is OEM software?

BCD

Bootmgr

Boot.ini was replaced by the BCD, which holds configuration data about which operating systems are installed. MSCONFIG is used to edit the BCD file.

If the screen on a CRT monitor is broken, you cannot reclaim any materials from it. If the CRT is intact, you can reclaim lead, mercury and phosphorus from it. You can reclaim metal from circuit boards and computer cases, you can also reclaim data from a hard drive, even if the data has been erased.

Grep Linux

Chmod linux

Ps linux

Apt-get linux

Learn all the hidden folders in Windows

Arp poisoning (spoofing)

SOE (standard operating environment)

What does increasing/decreasing the size of pagefile.sys do?

What does increasing/decreasing the size of win386.swp do?

WIN386.SWP

PAGEFILE.SYS

Winload.exe

bootmgr

hiberfil.sys

SmartScreen filter on Microsoft Edge

Material Safety Data Sheet (MSDS)

Wake on LAN is enabled through BIOS

The default permission position in a safe network should be implicit deny

You should return empty toner cartridges to the manufacturer for recycling

You can change your local password by pressing ctrl+alt+del and select Change a Password

Rainbow attack

Sfc utility

Which of the following authentication methods separates authentication and authorization into two different processes? TACACS?

Defrag /v

Gpupdate

Gpresult

You need to view the content of a Windows 10 update, what command line tool would you use?

Expand? Extract?

What does the $ stand for in Windows?

Regulated data and the privacy of electronic information in europe?

GPDR, PII, PCI, PHI

Is there a difference between flashing the bios and updating the EEPROM chip?

The difference between an implicit deny and an explicit deny /allow?

Active directory logical security concepts:

Folder redirection, login script, domain membership, organizational unit

What do you need to implement bitlocker to go on windows 7? What is bitlocker to go? It’s a technology in Windows 7 that allow you to encrypt the contents of USB flash drives.

REGSVR32 is used to register and unregister dll and Active X files in the registry.

A corrupt registry is solved by restoring the registry from a backup

Missing .exe files can be solved by application re-installation.

The boot.ini file was used in Windows xp, replaced by?...

The snap function to display two side-by-side applications can be done in Windows 7 and later

The difference between the services and startup tabs in msconfig

You cannot create a homegroup if the computer is already part of a domain

In order to return a Windows computer to its original setting, use the Factory recovery partition

Tools tab in hard drive properties, does not have format

What is a rainbow attack?

The factors that generate and promote the transmission of ESD are moving machines, moving people, improper grounding and humidity below 40%

How can you tell a shared folder is an administrative share?

Share permissions do not include read, write, modify and full control. They only include read, change and full control.

Homegroup only works on Windows 7, 8 and 8.1

Homegroup was removed in Windows 10

Windows commands you need to know for the exam:

Dir

Cd

Md

Ren

Rd

Deltree

Del

Tasklist

Taskkill

Shutdown

Sfc

bootrec

A user has a Windows 7 computer with 512 mb of ram and two hard drives, anmed drive C and D. The paging file is located on drive C. The user complains that his computer does not perform well after running for a couple hours. What should you tell the user to do? Move the paging file to drive D. **What does this mean?**

PowerShell Core 6.0 can be used on Windows 8 and later

A computer that is constantly being shut down improperly may negatively affect dll files

What are dll files?

What are BCD files?

The system restore feature is closely tied to the Volume Shadow Copy Service (VSS) in Win 7 and above. The feature is also disabled if VSS is disabled. VSS provides a mechanism for creating consistent point-in-time copies of data, known as shadow copies. System Restore allows you to use a restore point to return a system to a certain point in time.

If you want to increase the transmission area of a wireless access point increase the power level setting.

The only reason you would use WPA over WPA2 is with older wireless clients that do not support WPA2.

A trojan horse is malicious software that relies on other applications to execute and infect the system.

Confidentiality, integrity and availability, also known as the **CIA triad**, is a model designed to guide policies for information security within an organization. The model is also sometimes referred to as the AIC **triad** (availability, integrity and confidentiality) to avoid confusion with the Central Intelligence Agency.

You need to create a hard drive image on a Linux computer. Which command should you use?

Mv

Ls

Dd

Cp

What is the minimum free disk space needed to run defragmentation?

What three conditions affect the external vulnerabilities of wireless networks?

Access point power, antenna selection, antenna placement

As an IT technician, you should only report issues to your supervisor. If you find inappropriate material on a company owned computer and no specific acceptable use policy exists, inform your supervisor.

You need to take these security considerations into account then installing and configuring applications on Windows desktops: impact to device, user privileges, turning Windows features on or off.

The post-implementation impact a proposed change would have on the company workforce is covered in the “Documented business processes” section of the change request form.

“BOOTMGR is missing” is fixed by using an installation DVD and selecting “Automatic Repair” in the Advanced options menu.

The best way to decrease the amount of time it takes for Windows to startup and to increase the amount of available RAM on startup is to disable application startup.

Geotracking is not a security measure for mobile devices.