---

**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

Attrib windows command

Relative path vs direct path

List disk

An asterisk means its GPT, no asterisk means its MBR

**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.

Defrag /v

Gpupdate

Gpresult

Windows commands you need to know for the exam:

Dir

Cd

Md

Ren

Rd

Deltree

Del

Tasklist

Taskkill

Shutdown

Sfc

bootrec

---

**Windows Certification:**

Research these windows tools:

Memory diagnostics

Component services

Odbc data sources

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

What is Windows 8 RT?

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

So does Windows 7 Ultimate

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

Windows 7 can be upgraded to Windows 8 basic or pro

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

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

Perfmon and resmon

Learn all the hidden folders in Windows

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

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

**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.

Press F8 on boot in Windows 7 to enable System Recovery

The NTLDR was replaced by the boot.ini file

BCD

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

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

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

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

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

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.

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

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.

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

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.

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

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

SFC (System File Checker) utility

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

What does the $ stand for in Windows?

---

**Cybersecurity:**

**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

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

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

SmartScreen filter on Microsoft Edge

Material Safety Data Sheet (MSDS)

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

Rainbow attack

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

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.

What three conditions affect the external vulnerabilities of wireless networks?

Access point power, antenna selection, antenna placement

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

Software token and hardware tokens

RSA secure ID key fob

Like the google or blizz authenticator

User security vs data security

User authentication vs 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

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

Certificates

Effective access lists lets you 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

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

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

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

Firewalls are port security. Are there other forms of port security?

Regulated data and the privacy of electronic information in europe?

GPDR, PII, PCI, PHI

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

**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.

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.

---

**Linux commands:**

Redhat, fedora, centos: yum update

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

DD command

rsync is a utility for efficiently transferring and synchronizing files between a computer and an external hard drive and across networked computers by comparing the modification times and sizes of files. It is commonly found on Unix-like operating systems. Rsync is written in C as a single threaded application

Grep Linux

Chmod linux

Ps linux

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