Esentials of cyber security and cyber warfare

Syllabus and examination details

- TA 1 and 2 - 25 x 2 = 50
- MSE 01 - 50 x 1 = 50
- End semester examination = 100 marks

We need to work together to achieve goals.

Unit 1: windows security

- What U know about windows ?
- Your views on MS client operating system
- What about window server operating system ?
- Any other OS available in the market? Which r they ?
- Issues in windows 8.1/10/11
- Issues in Server OS.
- Which is the best operating system ? How ? Why ?

Windows security Infrastructure

https://cqureacademy.com/cyber-security-training/lvc-windows-security-infrastructure-management

What does security mean to microsoft ?

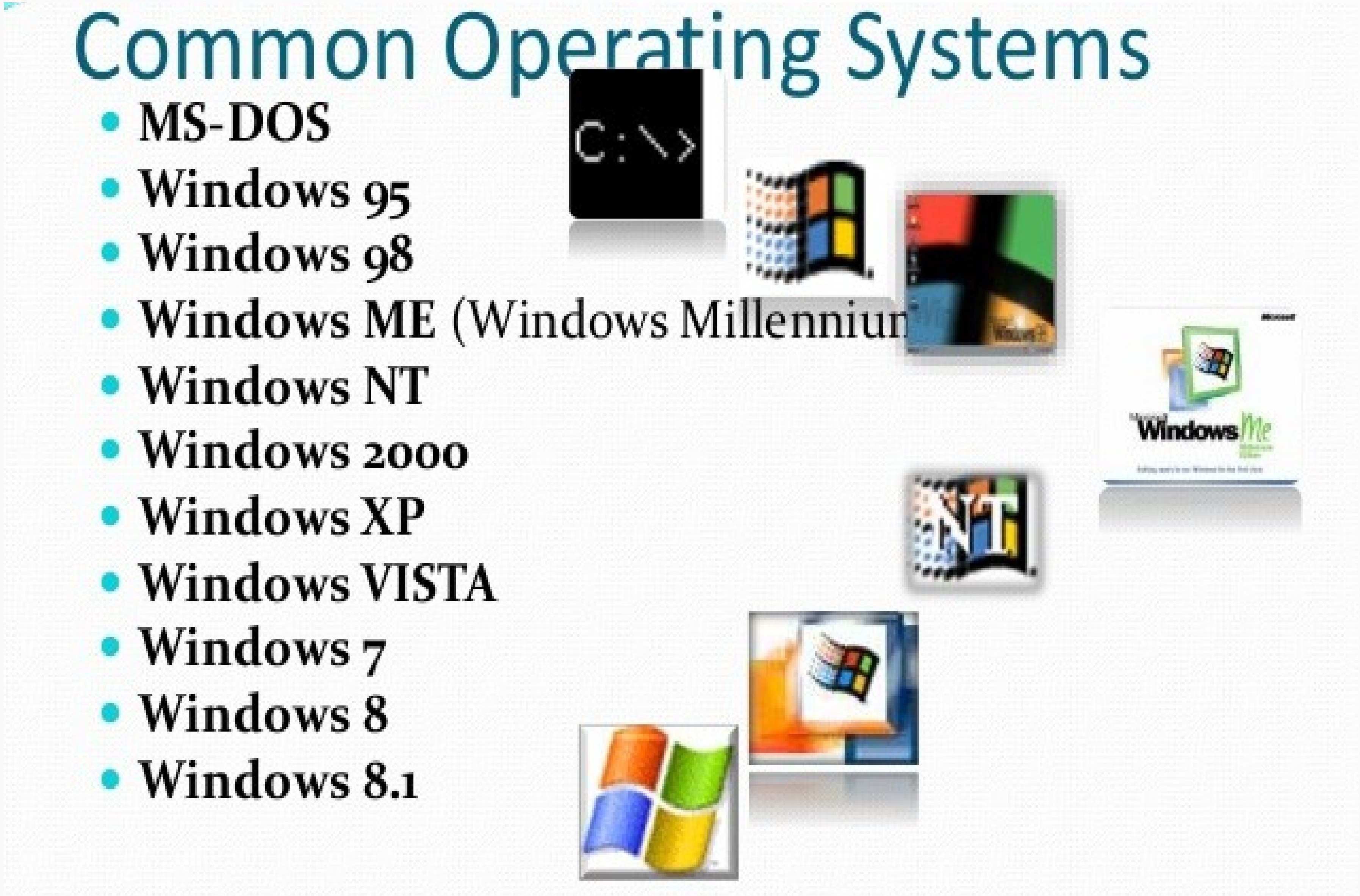
- Antivirus and scanning.
- Virus and threat protection.
- User Accounts protection.
- Firewall and network protection.
- Apps and browser control
- Device security
- Device performance and health.

Types/classification of operating system

- Single user
- Multi user
- Multi tasking
- Multi processing
- Embedded
- Realtime

https://www.geeksforgeeks.org/types-of-operating-systems/
https://www.javatpoint.com/types-of-os
https://afteracademy.com/blog/what-are-the-types-of-an-operating-system

Client Operating system



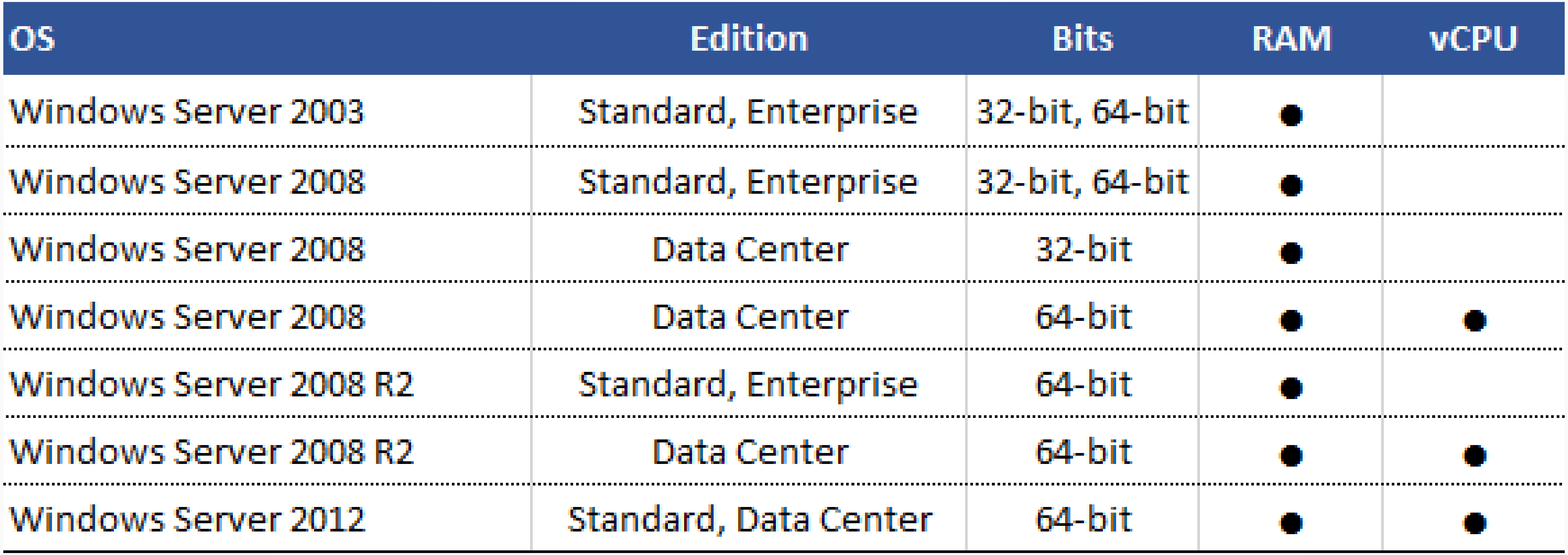
Common Operating Systems

- MS-DOS
- Windows 95
- Windows 98
- Windows ME (Windows Millenniu
- Windows NT
- Windows 2000
- Windows XP
- Windows VISTA
- Windows 7
- Windows 8
- Windows 8.1

What was the issues with each OS ?

How it is rectified in the next version of OS ?

Server Operating system



OS	Edition	Bits	RAM	vCPU
Windows Server 2003	Standard, Enterprise	32-bit, 64-bit	●	
Windows Server 2008	Standard, Enterprise	32-bit, 64-bit	●	
Windows Server 2008	Data Center	32-bit	●	
Windows Server 2008	Data Center	64-bit	●	●
Windows Server 2008 R2	Standard, Enterprise	64-bit	●	
Windows Server 2008 R2	Data Center	64-bit	●	●
Windows Server 2012	Standard, Data Center	64-bit	●	●

https://www.microsoft.com/en-in/windows-server

Embedded Operating system

https://blog.felgo.com/embedded/embedded-operating-systems

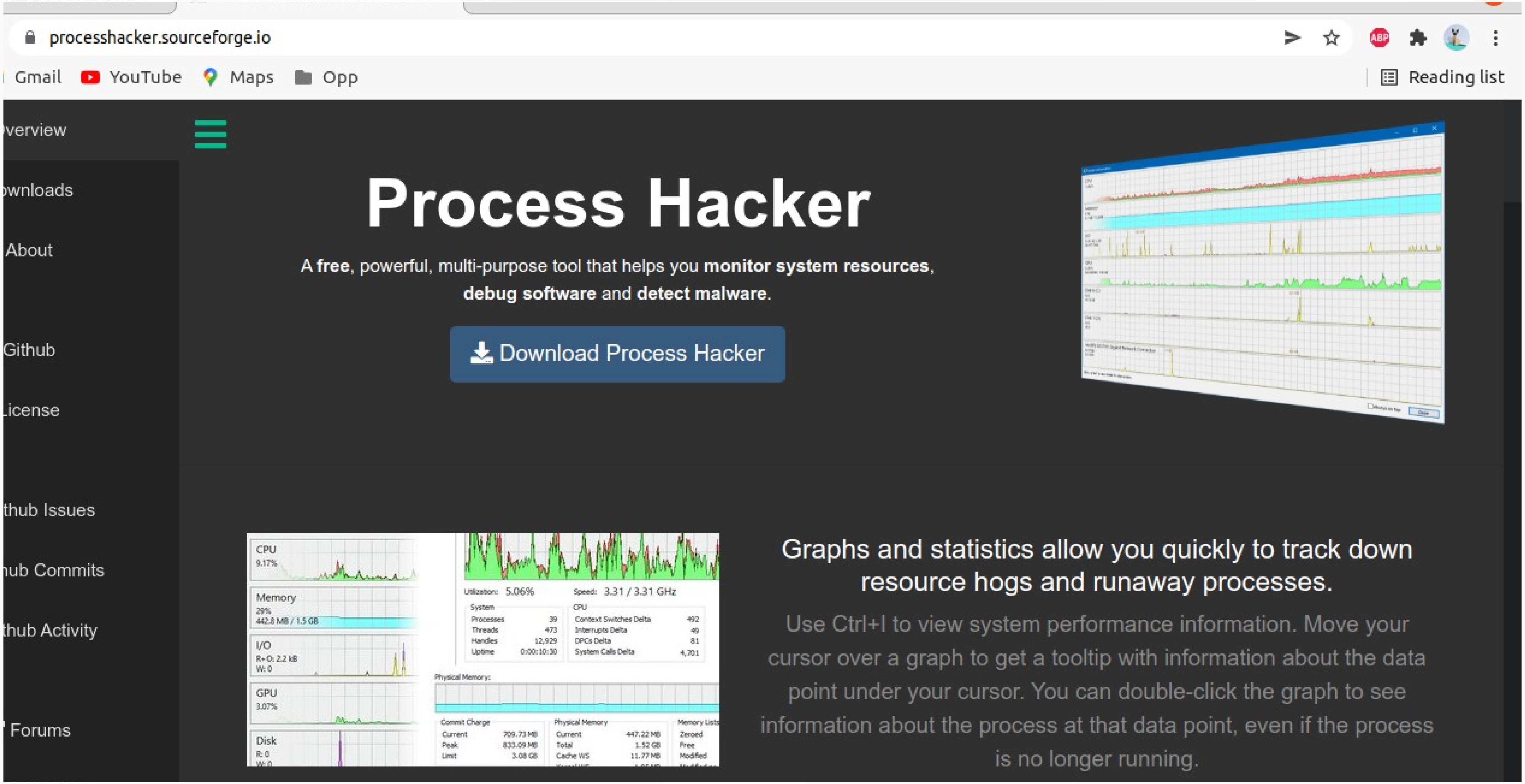
https://www.maxphi.com/embedded-operating-systems

https://www.qt.io/embedded-development-talk/essential-guide-to-embedded-operating-systems

https://www.nasa.gov/sites/default/files/482489main_4100_-_RTOS_101.pdf

https://www.cis.upenn.edu/~lee/06cse480/lec-rtos.pdf (an area to explore and present paper with contribution)

Practicals related to process hacking



Process Hacker

A **free**, powerful, multi-purpose tool that helps you **monitor system resources**, **debug software** and **detect malware**.

Graphs and statistics allow you quickly to track down resource hogs and runaway processes.

Use Ctrl+I to view system performance information. Move your cursor over a graph to get a tooltip with information about the data point under your cursor. You can double-click the graph to see information about the process at that data point, even if the process is no longer running.

Service packs

In computing, a service pack comprises a collection of updates, fixes, or enhancements to a software program delivered in the form of a single installable package.

Hot fixes

Hotfixes are different from regular updates and are not being offered or automatically installed via Windows Update. Hotfixes are intended to only fix a very specific issue (or set of issues) and usually have received less testing.

Backups

What is data backup ?

How to backup data ?

Where to backup data ?

When to backup data ?

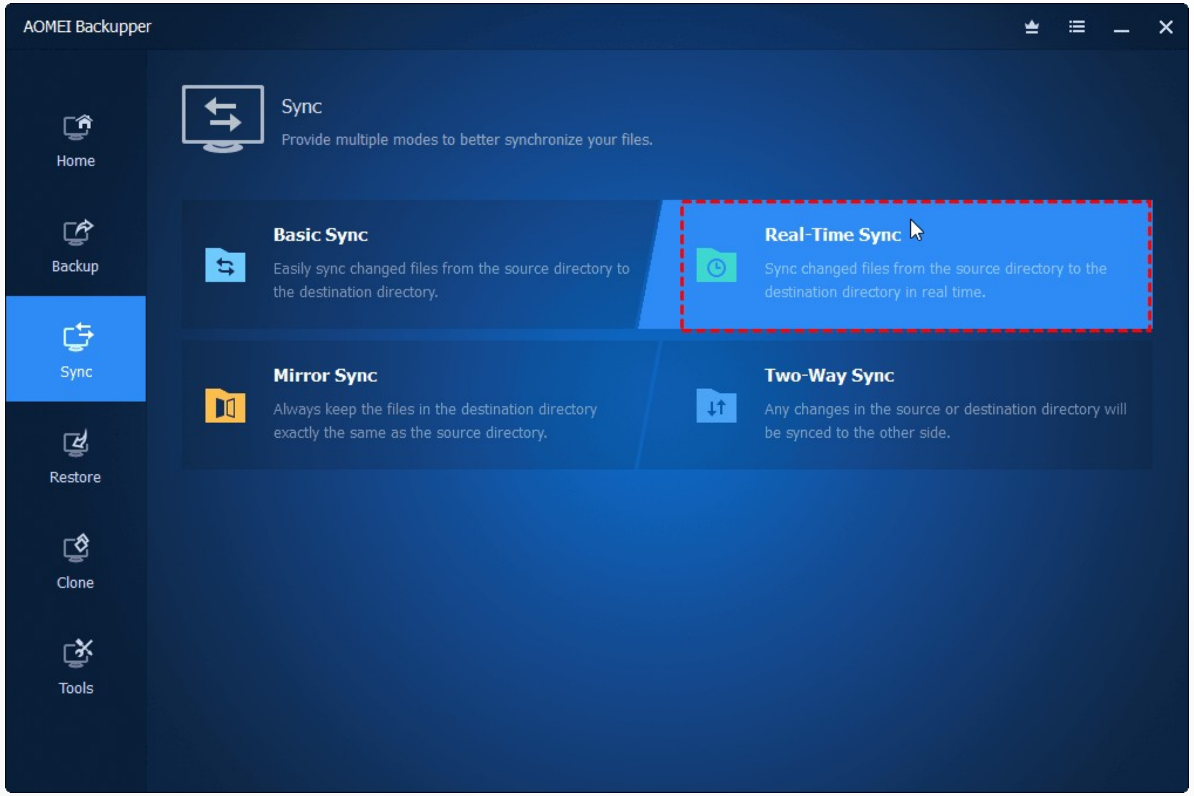
Why to backup data ?

Any backup devices available in the available system ?

Software helping data backup

How to backup realtime data ?

Backups Realtime Data



Sync

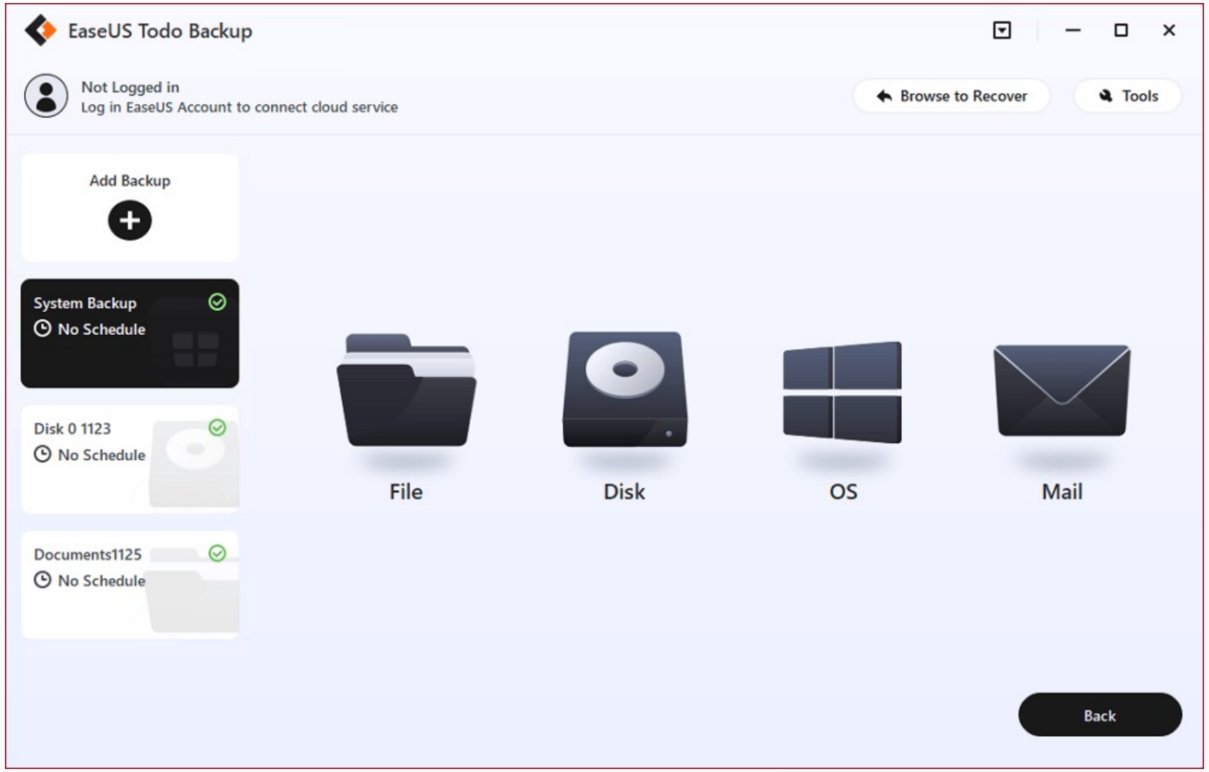
Provide multiple modes to better synchronize your files.

Basic Sync
Easily sync changed files from the source directory to the destination directory.

Real-Time Sync
Sync changed files from the source directory to the destination directory in real time.

Mirror Sync
Always keep the files in the destination directory exactly the same as the source directory.

Two-Way Sync
Any changes in the source or destination directory will be synced to the other side.



Not Logged in
Log in EaseUS Account to connect cloud service

System Backup
No Schedule

Disk 0 1123
No Schedule

Documents1125
No Schedule

Security bulletin

The Microsoft Security Response Center releases security bulletins on a monthly basis addressing security vulnerabilities in Microsoft software, describing their remediation, and providing links to the applicable updates for affected software. Each security bulletin is accompanied by one or more unique Knowledge Base Articles to provide further information about the updates.

https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2013/ms13-014

https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2003/ms03-048

https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2003/ms03-042

https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2007/ms07-056

https://www.qualys.com/research/security-alerts/2021-11-09/microsoft/

Patch Installations in windows

What is a patch ?

What is a need to have patch in any OS ?

How to install/Uninstall patch?

(https://www.watchguard.com/ help/docs/ help-center/en-us/content/en-us/endpoint-security/security-modules/patch-management/patch-management_install.html)

Automatic updates

What is automatic updates ?

How do i turn ON/ OFF automatic updates ?

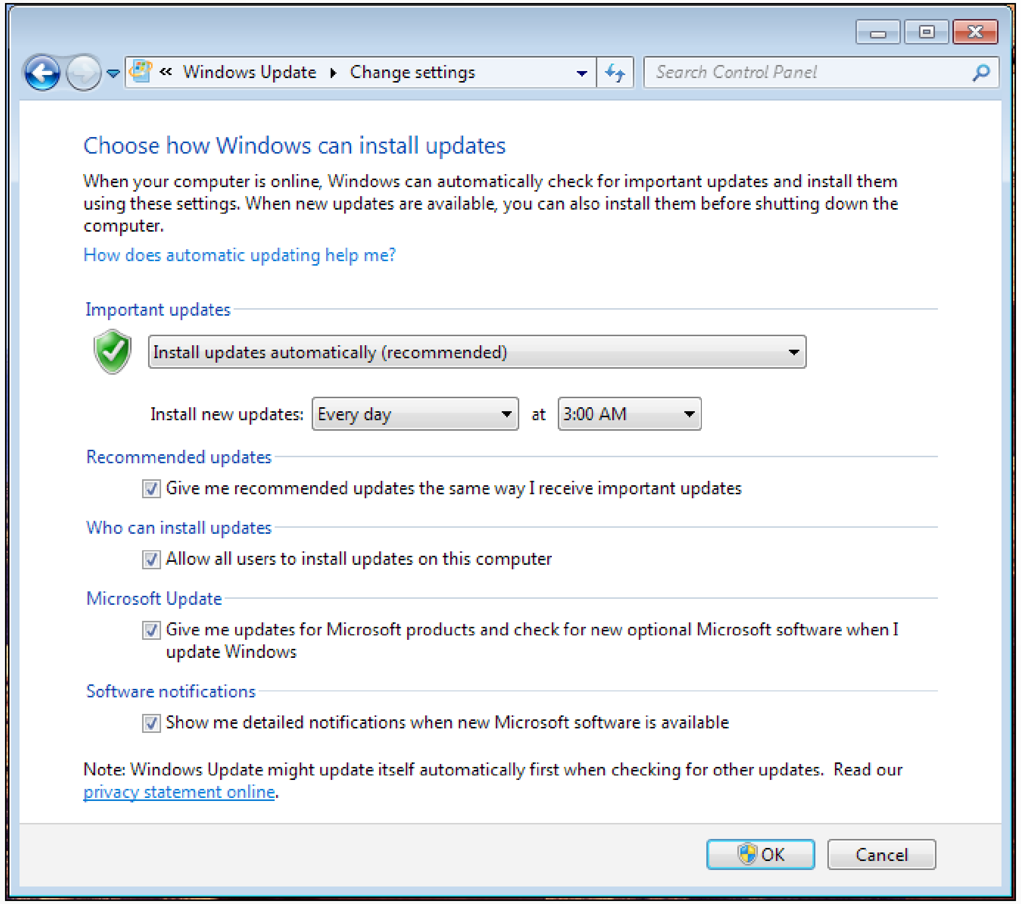
Do i need to check for updates ?

How much does it costs to update windows automatically ?

How do i know what updates have been installed ?

What can i do if i have any problem while installing updates ?

Automatic updates



Choose how Windows can install updates

When your computer is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also install them before shutting down the computer.

How does automatic updating help me?

Important updates

Install updates automatically (recommended)

Install new updates: Every day at 3:00 AM

Recommended updates

☑ Give me recommended updates the same way I receive important updates

Who can install updates

☑ Allow all users to install updates on this computer

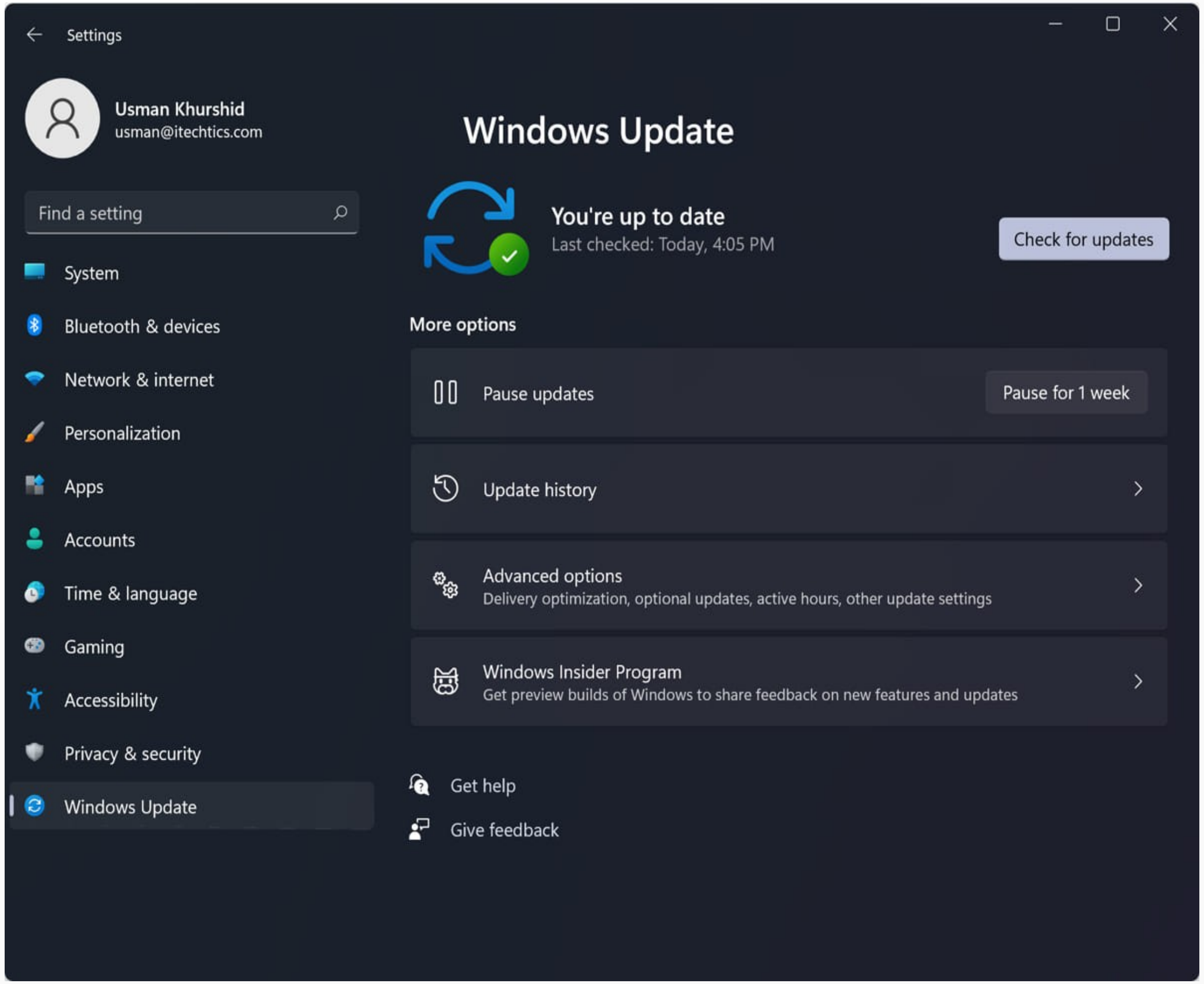
Microsoft Update

☑ Give me updates for Microsoft products and check for new optional Microsoft software when I update Windows

Software notifications

☑ Show me detailed notifications when new Microsoft software is available

Note: Windows Update might update itself automatically first when checking for other updates. Read our privacy statement online.



Windows Update

You're up to date

Last checked: Today, 4:05 PM

More options

Pause updates — Pause for 1 week

Update history

Advanced options
Delivery optimization, optional updates, active hours, other update settings

Windows Insider Program
Get preview builds of Windows to share feedback on new features and updates

Windows server update services

Windows Server Update Services (WSUS) is a free add-on application offered by Microsoft that can download and manage updates and patches for Windows Server operating systems.

How to configure windows server update services?

https://xpertstec.com/how-to-configure-windows-server-update-services-wsus/

About Windows server 2022

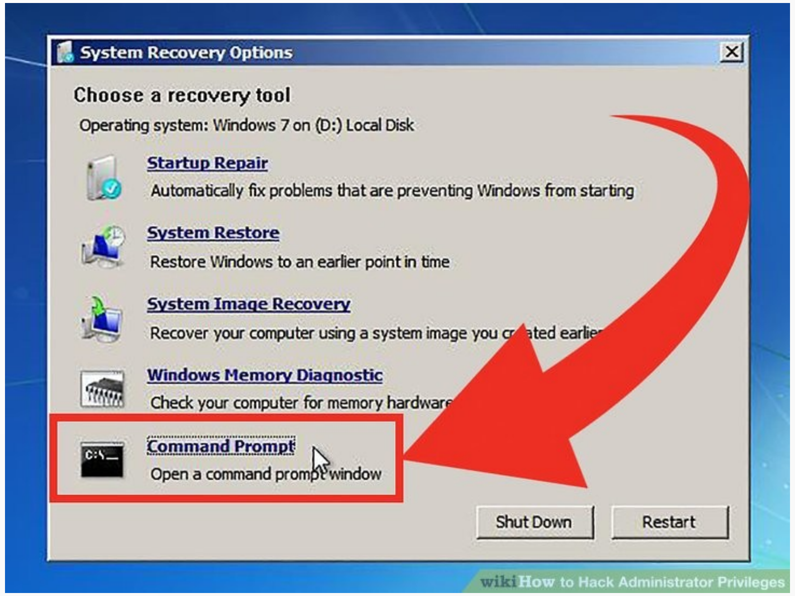
https://docs.microsoft.com/en-us/windows-server/get-started/whats-new-in-windows-server-2022

Windows backup and system restore

How to backup and restore data on windows 10/11 ?

What are the Challenges faced in the process

Reference:
https://support.microsoft.com/en-us/windows/back-up-and-restore-your-pc-ac359b36-7015-4694-de9a-c5eac1ce9d9c
https://www.windowscentral.com/how-make-full-backup-windows-10



Choose a recovery tool

Operating system: Windows 7 on (D:) Local Disk

Startup Repair
Automatically fix problems that are preventing Windows from starting

System Restore
Restore Windows to an earlier point in time

System Image Recovery
Recover your computer using a system image you cr ated earlie

Windows Memory Diagnostic
Check your computer for memory hardware

Command Prompt
Open a command prompt window

How to backup data on windows server 2019/2022 ?

What are the Challenges faced in the process

data backup in the cloud ?

Reference

https://appuals.com/how-to-perform-backup-and-restore-in-windows-server-2019/

Device driver rollback

How to rollback a drivers in windows ?

Need of driver rollback ?

Does your application is affected ?

Reference :

https://www.lifewire.com/how-to-roll-back-a-driver-in-windows-2619217

https://www.minitool.com/news/how-to-roll-back-a-driver.html

Windows Access Controls

Components of Access controls

- Authentication – password, digital certificate is used
- Authorization – office staff can view employee records
- Access – authorised person can access resources
- Manage – Manage system eg. Biometric login in office
- Audit -change of role in a company (clerk -> senior clerk)

Windows Access Controls

How does access control works ?

Physical access control: limits access to campuses, building and other physical assets, e.g. a proximity card to unlock a door.

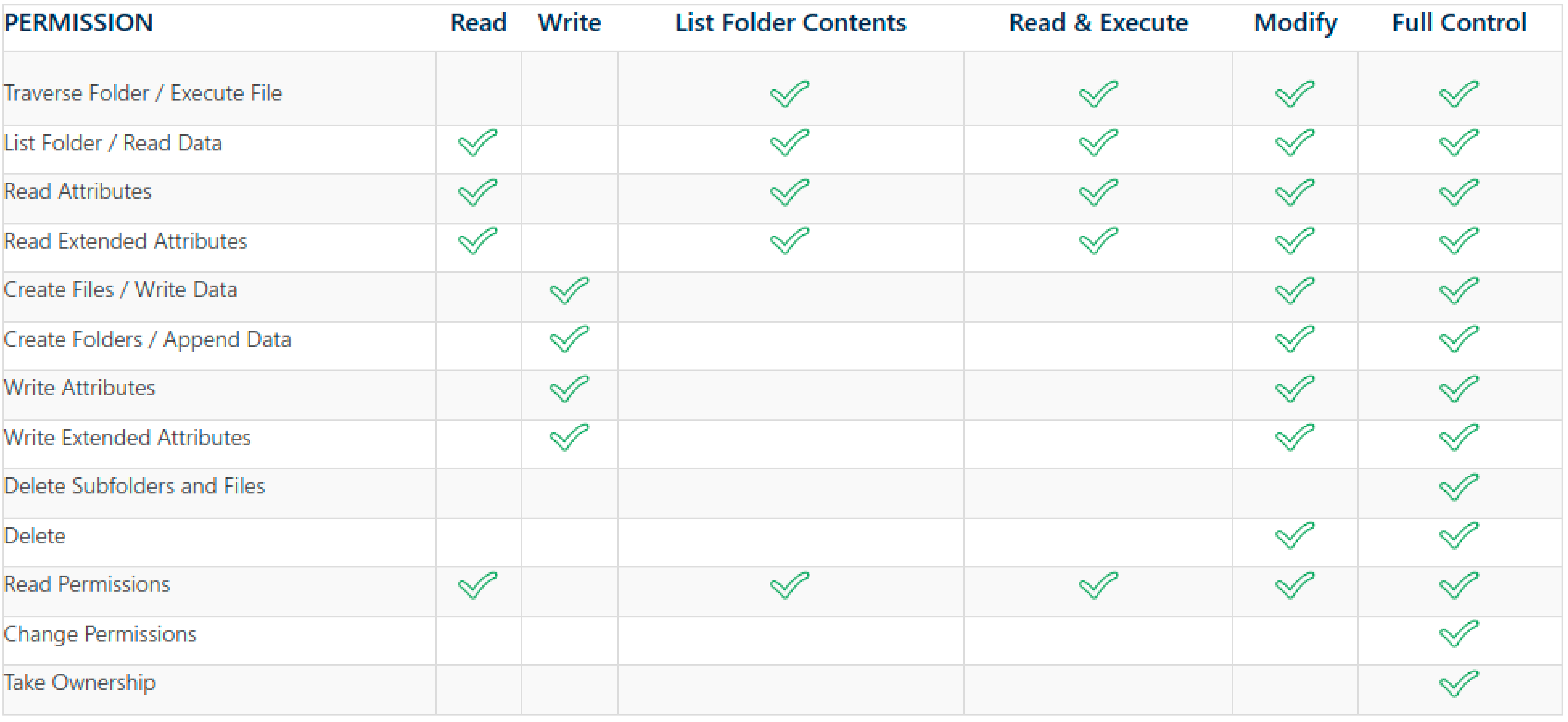
Logical access control: limits access to computers, networks, files and other sensitive data, e.g. a username and password.

Windows Access Controls

Types of Access controls ?   [relate with windows server]

- Attribute-based access control (ABAC)- 18 years of age for GF/BF.
- Discretionary access control (DAC) – each admin manage access rights - conflicts may occur at multiple levels.
- Mandatory access control (MAC) – used to protect highly sensitive data. Managed at central level.
- Role-based access control (RBAC) -access is controlled at the system level like in bank system.
- Rule-based access control – managed by admin like come at 9.50 am
- Break-Glass access control -follow principle of least previlage eg. Patient admitted in icu than only one person can visit the patient at certain time.

NTFS permissions



PERMISSION	Read	Write	List Folder Contents	Read & Execute	Modify	Full Control
Traverse Folder / Execute File			✓	✓	✓	✓
List Folder / Read Data	✓		✓	✓	✓	✓
Read Attributes	✓		✓	✓	✓	✓
Read Extended Attributes	✓		✓	✓	✓	✓
Create Files / Write Data		✓			✓	✓
Create Folders / Append Data		✓			✓	✓
Write Attributes		✓			✓	✓
Write Extended Attributes		✓			✓	✓
Delete Subfolders and Files						✓
Delete					✓	✓
Read Permissions	✓		✓	✓	✓	✓
Change Permissions						✓
Take Ownership						✓

NTFS permissions

File formats

How NTFS is different from FAT ?

How NTFS is different from FAT32 /ext4

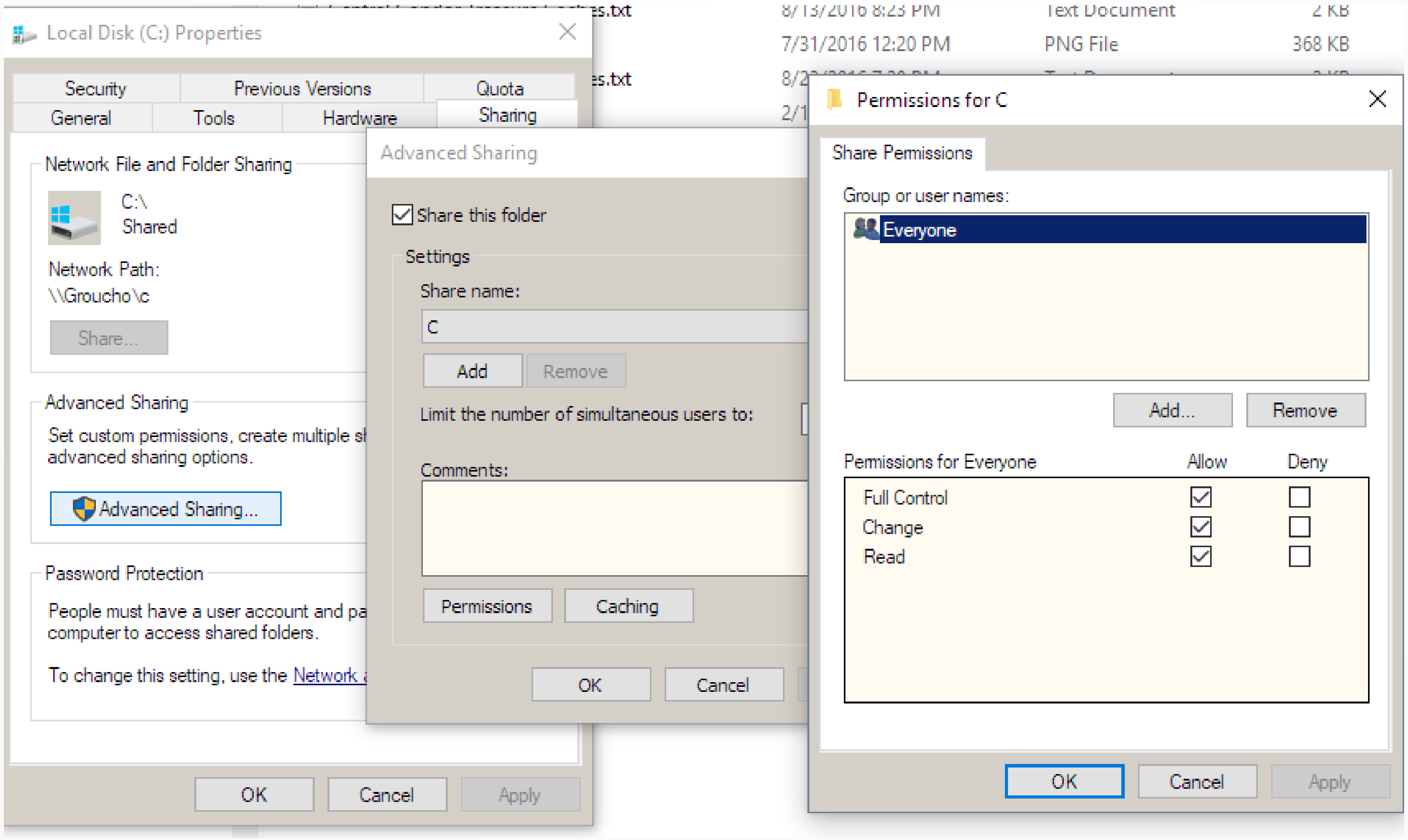
Shared Folder Permissions

What is shared folder permissions?

In Microsoft Windows, shared folder is a set of permissions that can be assigned to a shared folder to control access by users and groups on the network. Shared folder permissions can be applied only to the entire shared folder, not to its files and subfolders.

shared folder permissions are effective only when a user accesses the folder over the network.

Shared Folder Permissions



es.txt 8/13/2016 8:23 PM Text Document 2 KB

7/31/2016 12:20 PM PNG File 368 KB

es.txt

Local Disk (C:) Properties

Network File and Folder Sharing

C:\
Shared

Network Path:
\\Groucho\c

Advanced Sharing

Set custom permissions, create multiple sh
advanced sharing options.

Password Protection

People must have a user account and pa
computer to access shared folders.

To change this setting, use the Network a

Advanced Sharing

☑ Share this folder

Settings

Share name:

C

Limit the number of simultaneous users to:

Comments:

Permissions for C

Share Permissions

Group or user names:

Everyone

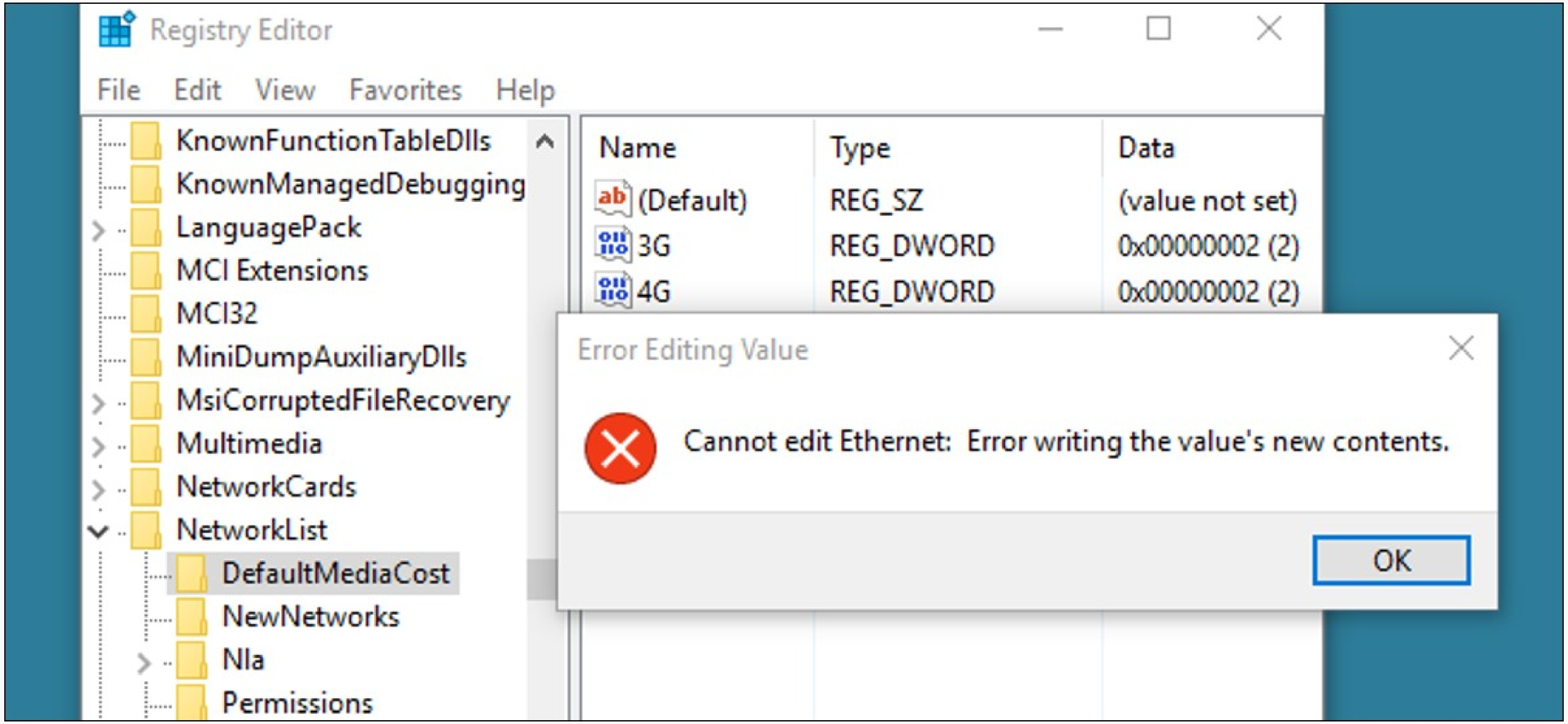
Permissions for Everyone	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

Reference : https://kb.synology.com/en-us/DSM/help/DSM/AdminCenter/file_share_privilege?version=6

Registry Key permissions

What are registry ?
Why you need permissions ?
How regedit.exe help in the process ?

Reference: https://www.howtogeek.com/262464/how-to-gain-full-permissions-to-edit-protected-registry-keys/



Name	Type	Data
ab (Default)	REG_SZ	(value not set)
3G	REG_DWORD	0x00000002 (2)
4G	REG_DWORD	0x00000002 (2)

Cannot edit Ethernet: Error writing the value's new contents.

Active Directory(AD) Permissions

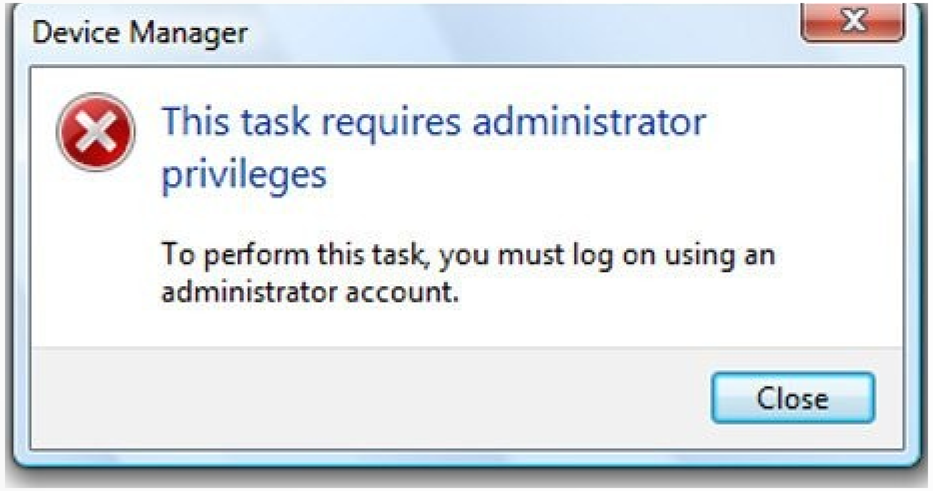
not all users need access to all the resources of the network. This is where AD permissions come into play. AD permissions ensure that users of an AD network only gain access to resources that they need. This prevents misuse of resources inside the network.

AD permissions are a set of rules that define how much an object has the authority to view or modify other objects and files in the directory.

permissions in AD are a security functionality. AD permissions are object-specific. When you assign permission to a container object, for example, you are given the control to restrict certain objects within the container not to inherit the permissions of the parent container.

Reference: https://www.youtube.com/watch?v=gdmq5qOrVck

Privileges



Device Manager

This task requires administrator privileges

To perform this task, you must log on using an administrator account.

A privilege is the right of an account, such as a user or group account, to perform various system-related operations on the local computer, such as shutting down the system, loading device drivers, or changing the system time.

Privileges

System Privileges for Object Types

CREATE TYPE - enables you to create object types in your own schema

CREATE ANY TYPE - enables you to create object types in any schema

ALTER ANY TYPE - enables you to alter object types in any schema

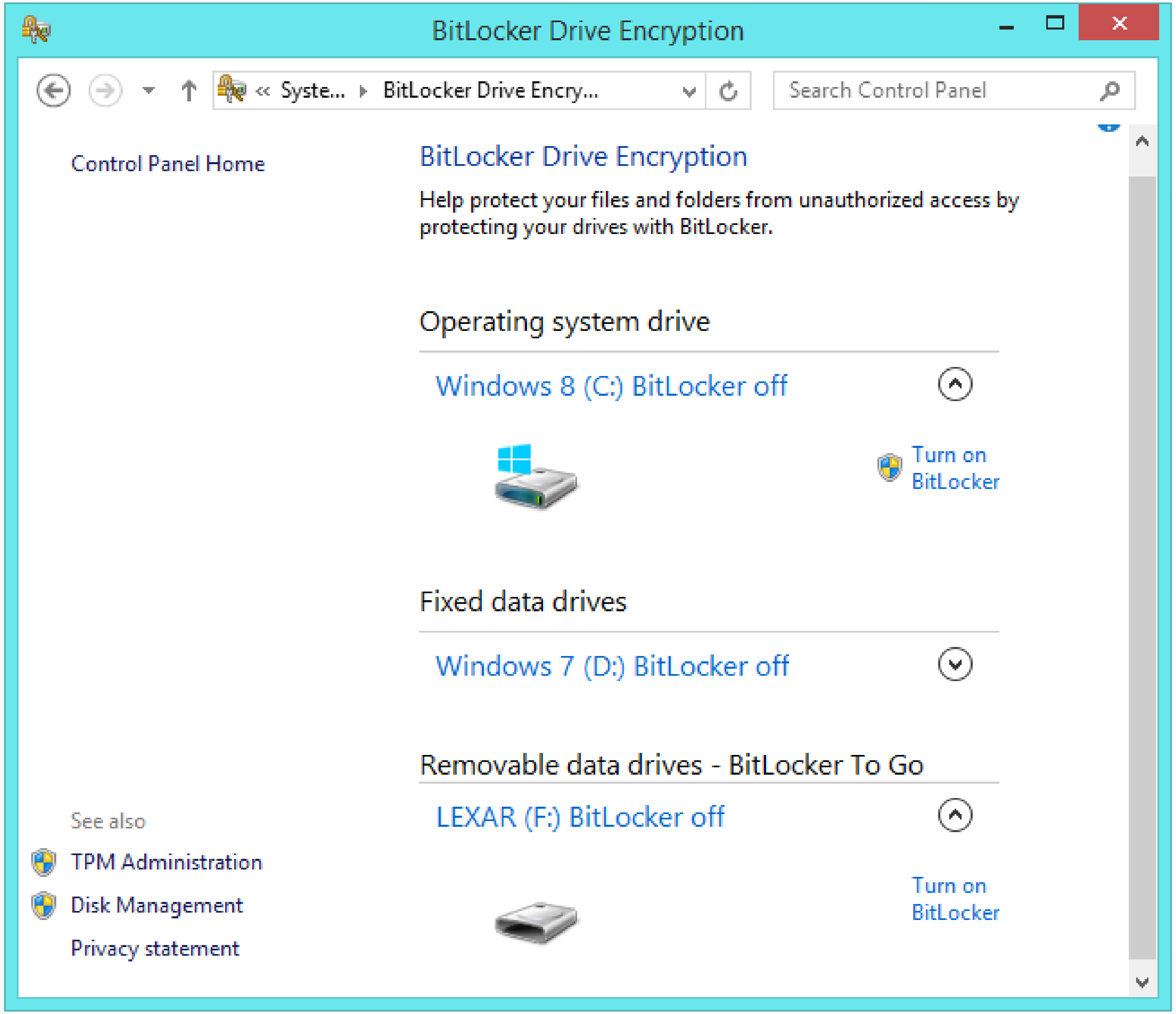
DROP ANY TYPE - enables you to drop named types in any schema

EXECUTE ANY TYPE - enables you to use and reference named types in any schema

UNDER ANY TYPE - enables you to create subtypes under any non-final object types

UNDER ANY VIEW - enables you to create subviews under any object view

BitLocker Drive Encryption



BitLocker Drive Encryption
« Syste... ▸ BitLocker Drive Encry...
Search Control Panel
Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

Windows 8 (C:) BitLocker off

Turn on BitLocker

Fixed data drives

Windows 7 (D:) BitLocker off

Removable data drives - BitLocker To Go

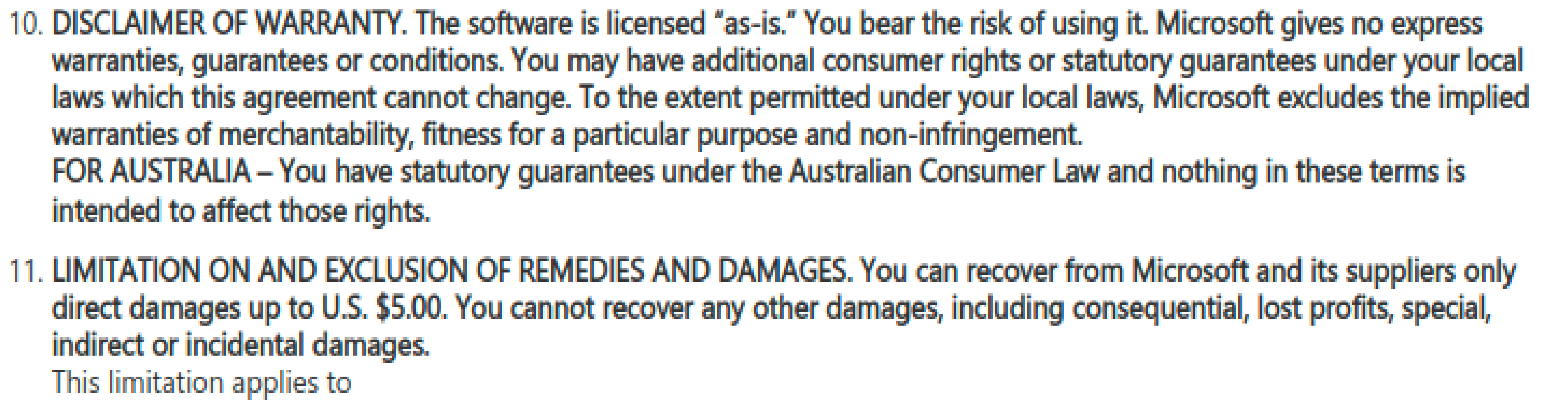
LEXAR (F:) BitLocker off

Turn on BitLocker

How to use bitlocker drive encryption ?

How to disable bitlocker ?

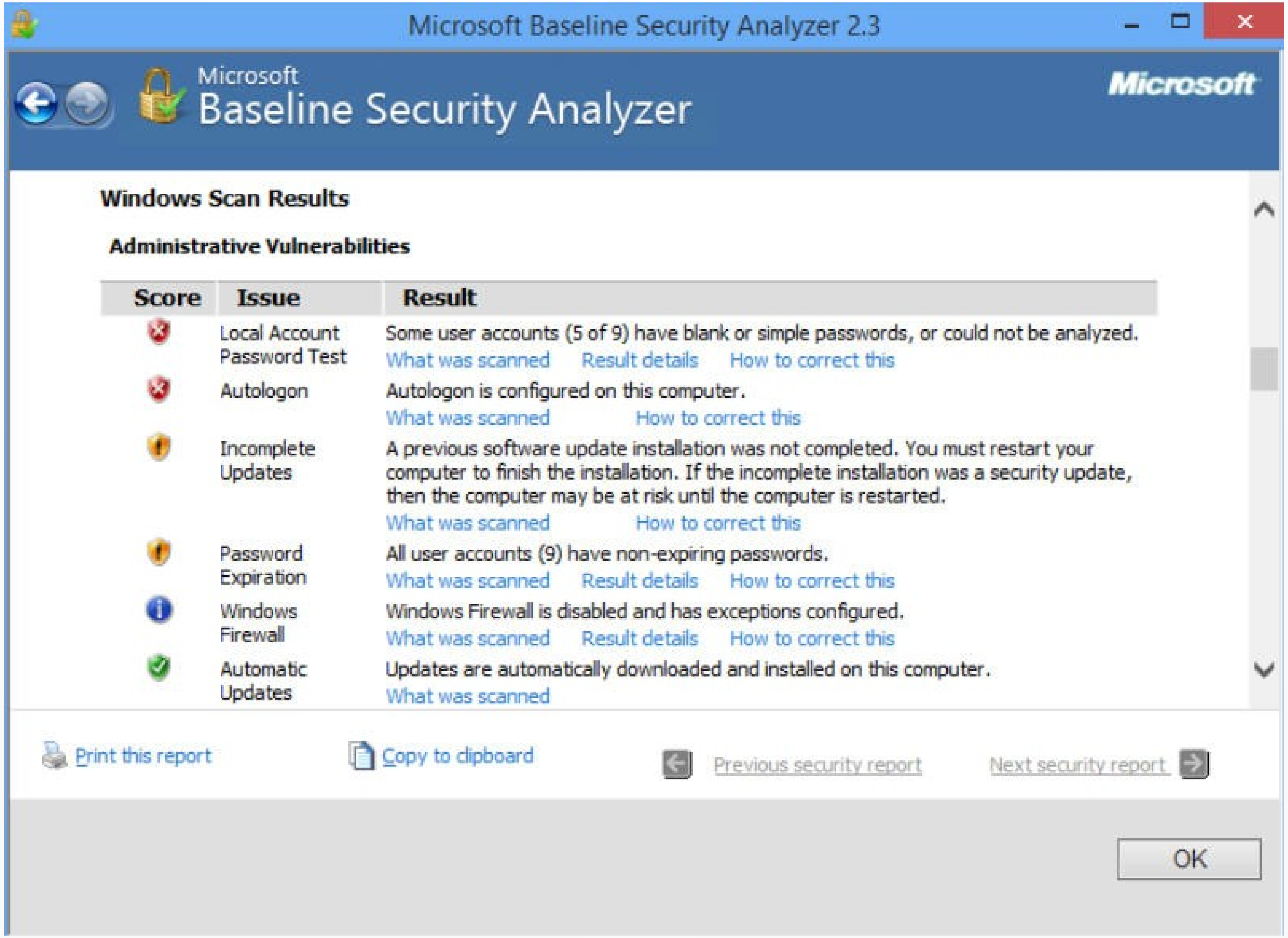
BitLocker Drive Encryption-warranty



10. DISCLAIMER OF WARRANTY. The software is licensed “as-is.” You bear the risk of using it. Microsoft gives no express warranties, guarantees or conditions. You may have additional consumer rights or statutory guarantees under your local laws which this agreement cannot change. To the extent permitted under your local laws, Microsoft excludes the implied warranties of merchantability, fitness for a particular purpose and non-infringement.
    FOR AUSTRALIA – You have statutory guarantees under the Australian Consumer Law and nothing in these terms is intended to affect those rights.

11. LIMITATION ON AND EXCLUSION OF REMEDIES AND DAMAGES. You can recover from Microsoft and its suppliers only direct damages up to U.S. $5.00. You cannot recover any other damages, including consequential, lost profits, special, indirect or incidental damages.
    This limitation applies to

Microsoft Baseline Security Analyzer



Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
✗	Local Account Password Test	Some user accounts (5 of 9) have blank or simple passwords, or could not be analyzed. What was scanned Result details How to correct this
✗	Autologon	Autologon is configured on this computer. What was scanned How to correct this
!	Incomplete Updates	A previous software update installation was not completed. You must restart your computer to finish the installation. If the incomplete installation was a security update, then the computer may be at risk until the computer is restarted. What was scanned How to correct this
!	Password Expiration	All user accounts (9) have non-expiring passwords. What was scanned Result details How to correct this
ℹ	Windows Firewall	Windows Firewall is disabled and has exceptions configured. What was scanned Result details How to correct this
✓	Automatic Updates	Updates are automatically downloaded and installed on this computer. What was scanned

Microsoft Baseline Security Analyzer

MBSA runs on Windows Vista, Windows Server 2003, Windows 2000, and Windows XP systems and will scan for common security misconfigurations in the following products:

Windows Vista, Windows 2000, Windows XP, Windows Server 2003, Internet Information Server (IIS) 5.0, and 6.0, SQL Server 7.0 and 2000, Internet Explorer (IE) 5.01 and later, and Office 2000, 2002 and 2003.

MBSA also scans for missing security updates, update rollups and service packs published to Microsoft Update.

CURRENTLY OUTDATED

Microsoft Baseline Security Analyzer

Alternative to MBSA

- SolarWinds Network Configuration Manager
- Open Vulnerability Assessment System
- Nexpose Community Edition
- Retina Network Community

Home work for submission

- Compare windows client OS (Windows XP,7,8.1 and 11)
- How Ubuntu 20.04 LTS is different from windows 11?
- Compare lates window server 2022 with Linux server.
- Elaborate on Embedded OS.
- How Embedded OS is different from Realtime OS ?
- How to backup/migrate data on cloud platform ? Explain process with eg.
- Use any two tools to backup data from client OS.
- Use access controls on windows server 2022 and Linux Os.
- Install ubuntu 21.10 as client OS.
- Install server 2022 and manage access controls.
- Identify and install alternative to BitLocker.

Thank you for your contribution