Windows Fundamentals

Course Incharge: **Yahya Batla**

Course Instructor: **Umar Bilal**

Question?

1) Which OS do you think is the most secure?

-> MAC OS, due to being very hardened.

Question?

2) Which OS do you think should have been the most secure?

-> Windows OS has historically faced more security challenges due to its widespread usage and being a prime target for malware and cyberattacks. While recent versions have improved security measures, some still perceive it as less secure compared to other options.

Question?

Which OS do you think is the least secure?

-> It's not accurate to label any particular OS as the least secure universally. Each operating system has its strengths and weaknesses regarding security. However, some might argue that outdated or poorly maintained versions of any OS could be more vulnerable.

Windows History

- The Windows operating system, originating in 1985, dominates both home and corporate networks.
- Due to its widespread use, Windows has consistently been targeted by hackers and malware creators.
- Windows XP, a popular version, had a lengthy lifespan before the introduction of Windows Vista.
- Windows Vista, a significant overhaul, faced numerous issues and was poorly received by users.

Windows History continued…

- Upon Microsoft's announcement of the end-of-life for Windows XP, panic ensued among users, prompting a rush to adopt the next viable option, Windows 7.

- Vendors raced against time to ensure compatibility of their products with Windows 7, as customers sought compatible solutions.

- Windows 7 eventually faced its end-of-support date, leading to the introduction of Windows 8.x, which had a brief tenure similar to Vista.

- Then arrived Windows 10, which comes in 2 flavors, Home and Pro.

WINDOWS 10 HOME

- Typically cheaper, suitable for home users and consumers.
- Lacks BitLocker but includes basic security features like Windows Defender Antivirus.
- Does not include these features, less suitable for business environments.
- Can only connect to remote desktop sessions.
- Does not include Hyper-V.
- Less control, updates are generally required to install immediately.
- Cortana cannot be disabled.

WINDOWS 10 PRO

- Usually more expensive, targeted towards businesses and power users.
- Offers BitLocker encryption for entire hard drive protection.
- Includes domain join and group policy management for business networks.
- Can host remote desktop sessions.
- Includes Hyper-V for running virtual machines.
- More control over updates, including deferring and choosing when to install.
- Option to disable Cortana.

Windows 11

As of October 5th, 2021 - Windows 11 now is the current Windows operating system for end-users.

Read more about Windows 11 here:

https://www.microsoft.com/en-us/windows?wa=wsignin1.0

Windows Filesystems

- The file system used in modern versions of Windows is the New Technology File System or simply NTFS.
- Before NTFS, there was FAT16/FAT32 (File Allocation Table) and HPFS (High Performance File System).
- NTFS (New Technology File System) and FAT16/32 (File Allocation Table) are two different file systems used in Windows operating systems, each with its own set of features and capabilities

NTFS

- Advanced structure with features like journaling, file permissions, encryption, compression, and disk quotas.
- Supports larger file and volume sizes, up to 16 exabytes.
- Supports a wide range of attributes like file permissions, encryption, compression, and disk quotas.
- Advanced security features including access control lists (ACLs) and file-level encryption.
- Includes journaling for improved reliability and faster recovery in case of system crashes or power failures.

FAT16/32

- Simpler structure, lacking advanced features, primarily for basic file storage.
- Limited file size (up to 4 GB for FAT16, 4 GB - 1 byte for FAT32) and volume size (up to 4 GB for FAT16, 2 TB for FAT32).
- Limited support for basic attributes such as read-only, hidden, system, and archive.
- Lacks advanced security features, limited support for file permissions.
- Lacks journaling support, more prone to corruption and data loss in unexpected shutdowns or errors.

Windows Filesystem continued…

You still see FAT partitions in use today. For example, you typically see FAT partitions in USB devices, MicroSD cards, etc. but traditionally not on personal Windows computers/laptops or Windows servers.

You can read Microsoft's official documentation on FAT, HPFS, and NTFS here:

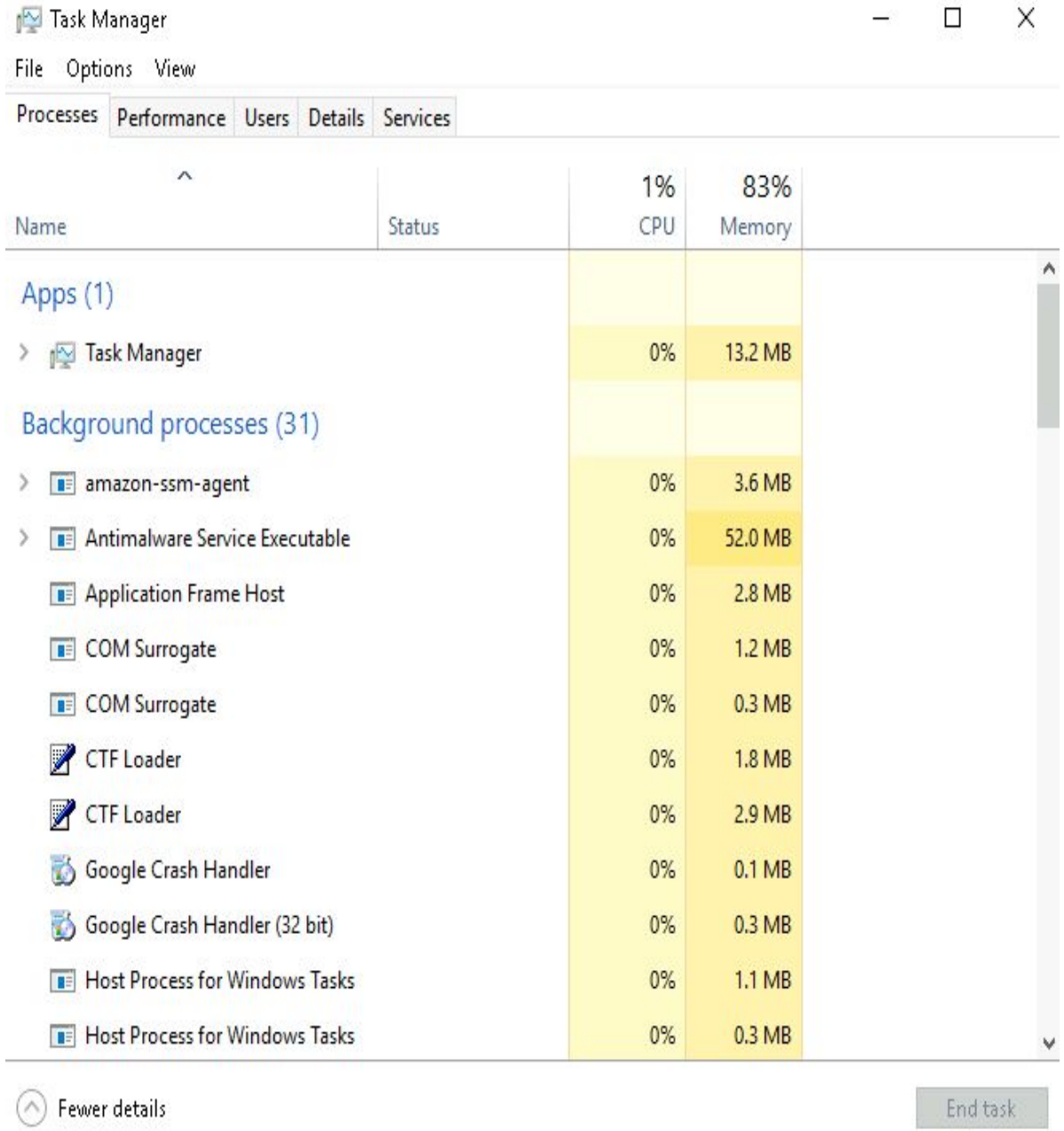
https://learn.microsoft.com/en-us/troubleshoot/windows-client/backup-and-storage/fat-hpfs-and-ntfs-file-systems

Essential Windows Components

- **Windows Directory:** The Windows folder (traditionally C:\Windows) houses the Windows operating system.
- It's not confined to the C drive; it can exist on any other drive or within another folder.
- System environment variables, like %windir%, are crucial here.
- According to Microsoft, environment variables contain OS environment details, like the OS path, processor count, and temporary folder location.

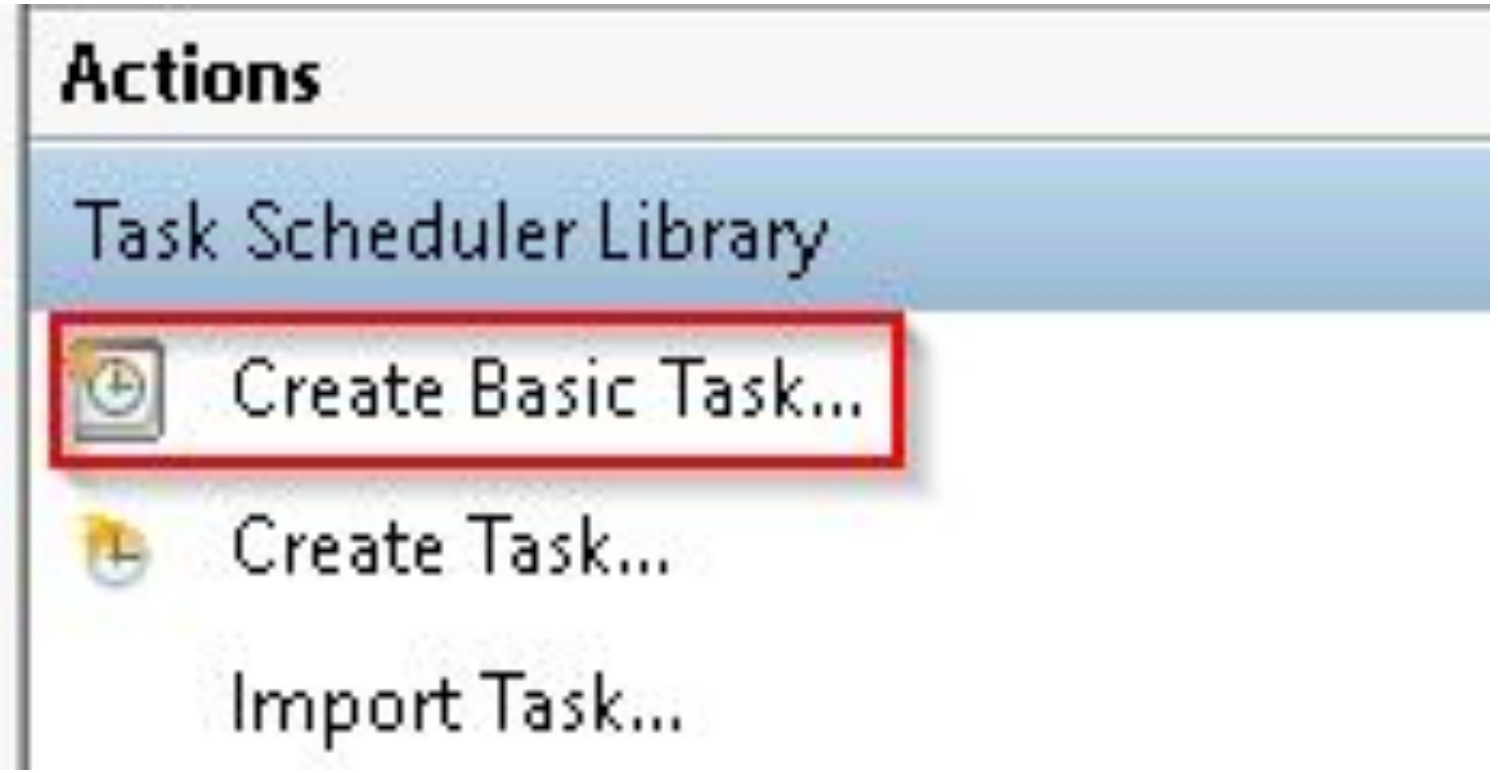
Essential Windows Components continued…

- **Task Manager:** Displays running applications and processes.
- Provides CPU and RAM usage information.
- Includes Performance section for detailed CPU and RAM utilization data.


Task Manager
File Options View
Processes Performance Users Details Services
Name Status 1% CPU 83% Memory
Apps (1)
Task Manager 0% 13.2 MB
Background processes (31)
amazon-ssm-agent 0% 3.6 MB
Antimalware Service Executable 0% 52.0 MB
Application Frame Host 0% 2.8 MB
COM Surrogate 0% 1.2 MB
COM Surrogate 0% 0.3 MB
CTF Loader 0% 1.8 MB
CTF Loader 0% 2.9 MB
Google Crash Handler 0% 0.1 MB
Google Crash Handler (32 bit) 0% 0.3 MB
Host Process for Windows Tasks 0% 1.1 MB
Host Process for Windows Tasks 0% 0.3 MB
Fewer details
End task

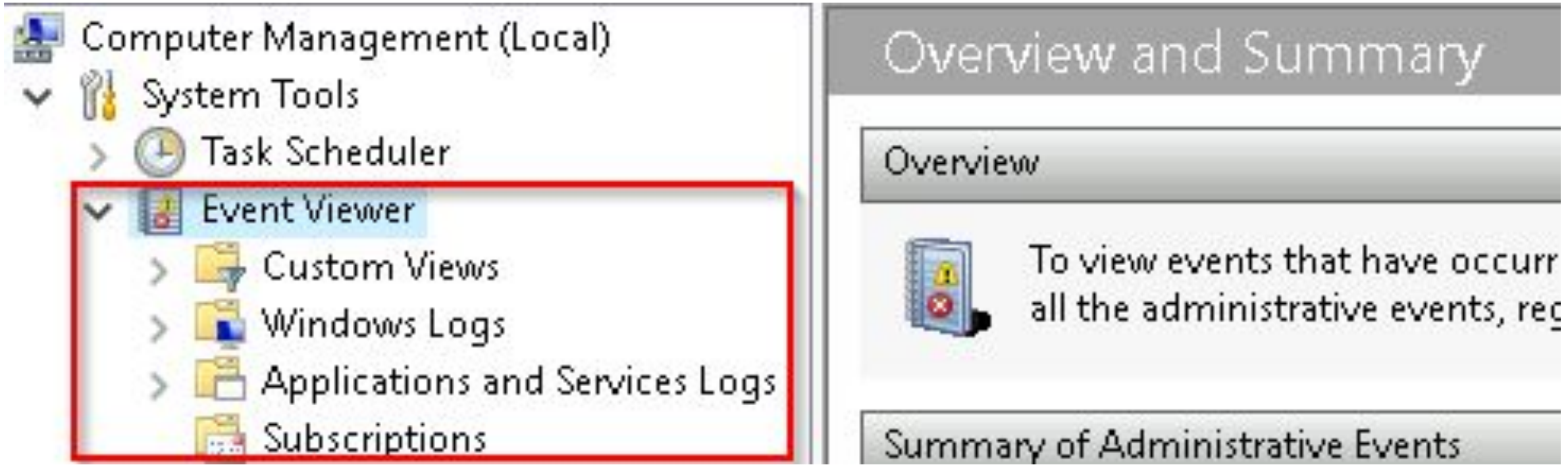
Essential Windows Components continued…

- **Task Scheduler:** Allows creation and management of automated tasks.
- Tasks can execute applications, scripts, etc.
- Can be scheduled for specific times or events like log in or log off.
- Offers flexible scheduling options, such as intervals (e.g., every five minutes).


Actions
Task Scheduler Library
Create Basic Task...
Create Task...
Import Task...

Essential Windows Components continued…

- **Event Viewer:** Displays computer system events.
- Acts as an audit trail for system activity understanding.
- Used for problem diagnosis and investigation of system actions.
- Five types of events can be logged.


Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Custom Views
Windows Logs
Applications and Services Logs
Subscriptions
Overview and Summary
Overview
To view events that have occurr
all the administrative events, reg
Summary of Administrative Events

The following table describes the five event types used in event logging.

Event type	Description
Error	An event that indicates a significant problem such as loss of data or loss of functionality. For example, if a service fails to load during startup, an Error event is logged.
Warning	An event that is not necessarily significant, but may indicate a possible future problem. For example, when disk space is low, a Warning event is logged. If an application can recover from an event without loss of functionality or data, it can generally classify the event as a Warning event.
Information	An event that describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, it may be appropriate to log an Information event. Note that it is generally inappropriate for a desktop application to log an event each time it starts.
Success Audit	An event that records an audited security access attempt that is successful. For example, a user's successful attempt to log on to the system is logged as a Success Audit event.
Failure Audit	An event that records an audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt is logged as a Failure Audit event.

Essential Windows Components continued…

Command Prompt (cmd):

- Initially the sole interface for operating systems.
- GUI introduced for easier task execution.
- GUI remains primary but cmd still functional.

Basic Commands:

- hostname: Outputs computer name.
- whoami: Outputs logged-in user name.
- ipconfig: Shows network address settings.
- /?: Retrieves help manual for a command.
- cls: Clears command prompt screen.

Essential Windows Components continued…

Advanced Commands:

- netstat: Displays protocol statistics and network connections. Parameters like -a, -b, -e alter output.
- net: Manages network resources, supports sub-commands. Typing 'net' without sub-commands shows syntax and available sub-commands.

Windows Security Features

Trusted Platform Module (TPM):

- Hardware-based technology for security functions.
- TPM chip: Secure crypto-processor for cryptographic operations.
- Incorporates multiple physical security mechanisms.
- Tamper-resistant design prevents manipulation by malicious software.

Windows Security Features continued…

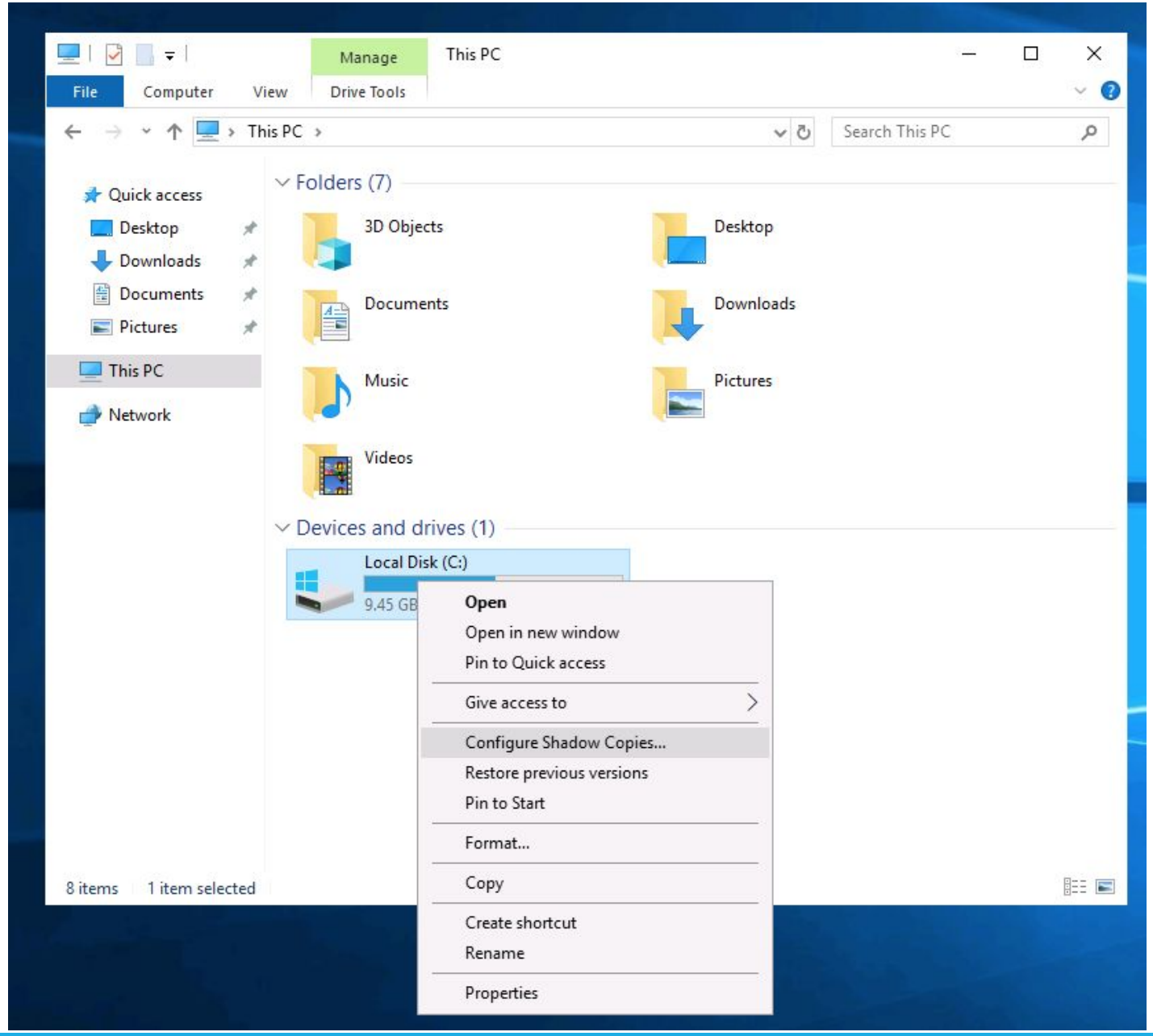
BitLocker:

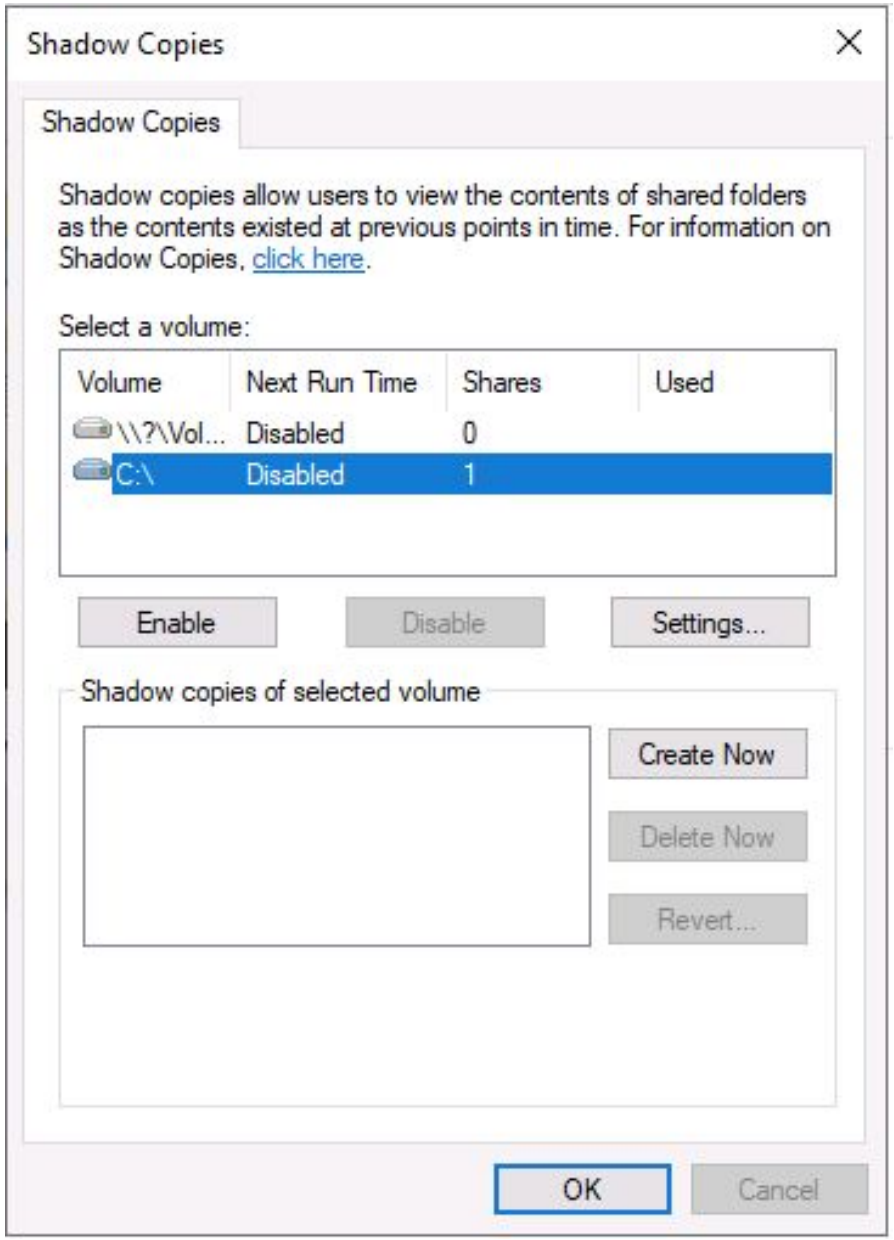
- Data protection feature integrated with the operating system.
- Addresses threats of data theft or exposure from lost, stolen, or decommissioned computers.
- Offers best protection on devices with TPM installed.
- Utilizes Trusted Platform Module (TPM) version 1.2 or later for enhanced security.
- TPM, a hardware component in newer computers, works with BitLocker to safeguard user data and detect offline tampering.

Windows Security Features continued…

Volume Shadow Copy Service:

- Per Microsoft, the Volume Shadow Copy Service (VSS) coordinates the required actions to create a consistent shadow copy (also known as a snapshot or a point-in-time copy) of the data that is to be backed up.
- Volume Shadow Copies are stored on the System Volume Information folder on each drive that has protection enabled.
- If VSS is enabled (System Protection turned on), you can perform the following tasks from within advanced system settings.
  - Create a restore point
  - Perform system restore
  - Configure restore settings
  - Delete restore points


Manage
This PC
File
Computer
View
Drive Tools
This PC
Search This PC
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Folders (7)
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Devices and drives (1)
Local Disk (C:)
9.45 GB
Open
Open in new window
Pin to Quick access
Give access to
Configure Shadow Copies...
Restore previous versions
Pin to Start
Format...
Copy
Create shortcut
Rename
Properties
8 items
1 item selected


Shadow Copies
Shadow Copies
Shadow copies allow users to view the contents of shared folders as the contents existed at previous points in time. For information on Shadow Copies, click here.
Select a volume:
Volume
Next Run Time
Shares
Used
\\?\Vol...
Disabled
0
C:\
Disabled
1
Enable
Disable
Settings...
Shadow copies of selected volume
Create Now
Delete Now
Revert...
OK
Cancel

Windows Security Features continued…

From a security perspective, malware writers know of this Windows feature and write code in their malware to look for these files and delete them. Doing so makes it impossible to recover from a ransomware attack unless you have an offline/off-site backup.

If you wish to interact hands-on with VSS, I suggest exploring Day 23 of Advent of Cyber 2:

- https://tryhackme.com/room/adventofcyber2

Practice!

Students are advised to complete the following TryHackMe room from their own THM account:

https://tryhackme.com/room/windowsfundamentals2x0x?path=undefined

https://tryhackme.com/room/windowsfundamentals3xzx?path=undefined

THANK YOU