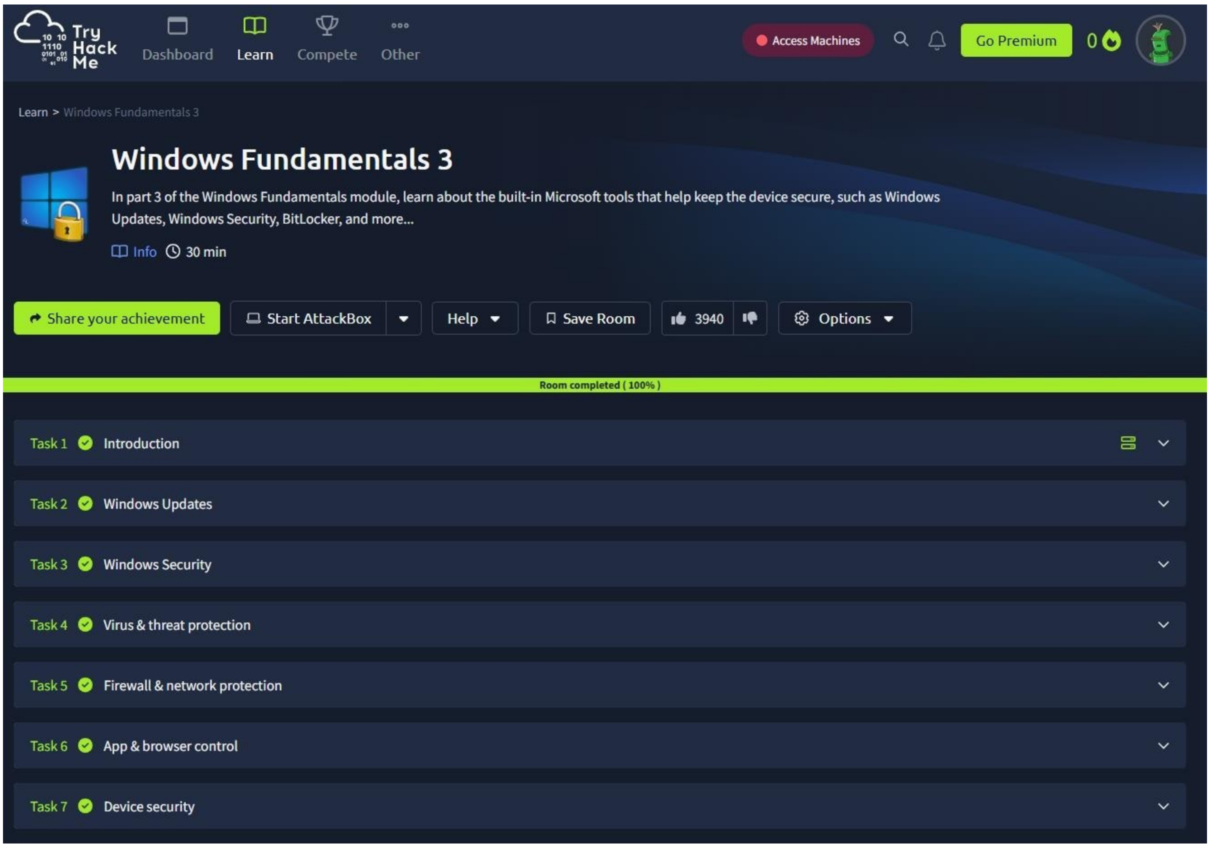
231901005

WINDOWS FUNDAMENTALS – 3

Aim: To provide an overview of the security features within the windows operating system.

Procedure:

- Introduction
- Windows Updates
- Windows Security
- Virus & Threat Protection
- Firewall & Network Protection
- App & Browser Control
- Device Security
- BitLocker
- Volume Shadow Copy Service
- Conclusion



Learn > Windows Fundamentals 3

Windows Fundamentals 3

In part 3 of the Windows Fundamentals module, learn about the built-in Microsoft tools that help keep the device secure, such as Windows Updates, Windows Security, BitLocker, and more...

Info 30 min

Room completed (100%)

Task 1 ✓ Introduction

Task 2 ✓ Windows Updates

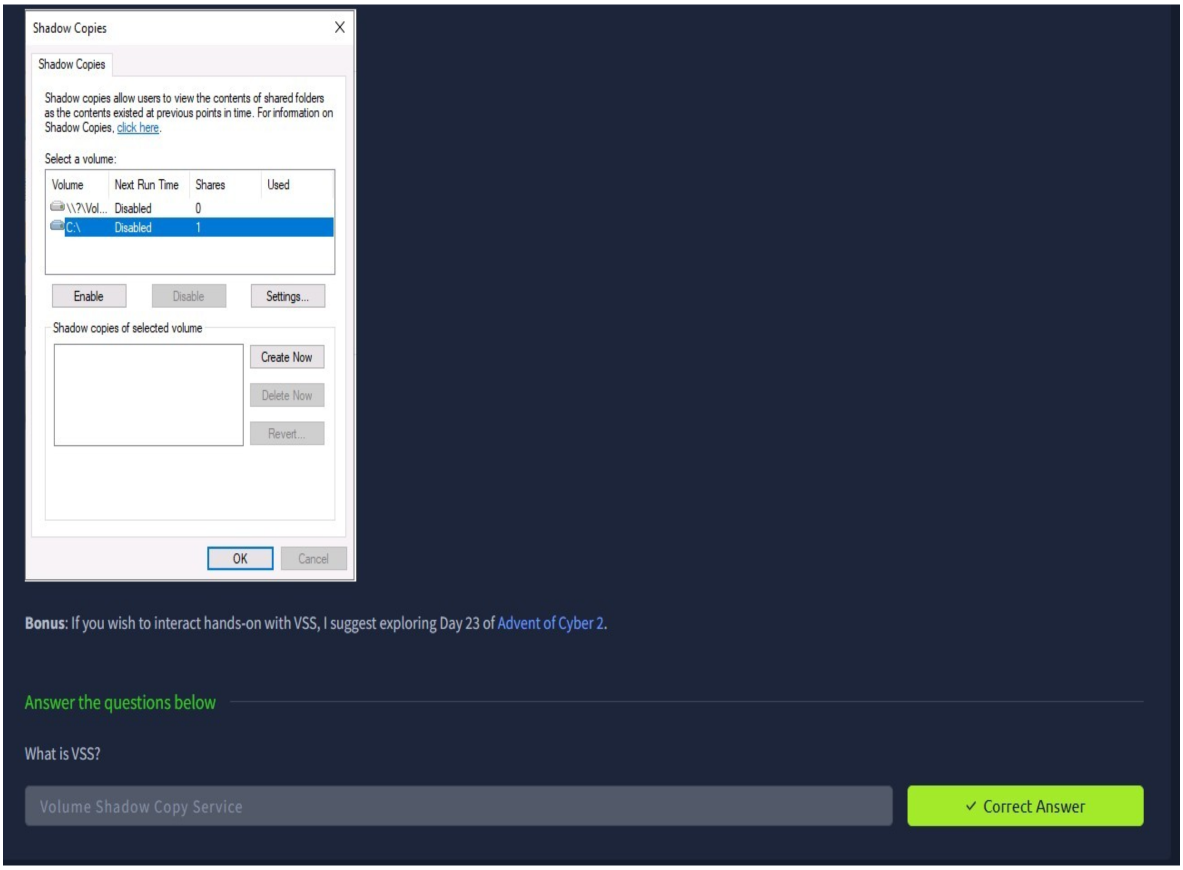
Task 3 ✓ Windows Security

Task 4 ✓ Virus & threat protection

Task 5 ✓ Firewall & network protection

Task 6 ✓ App & browser control

Task 7 ✓ Device security



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:

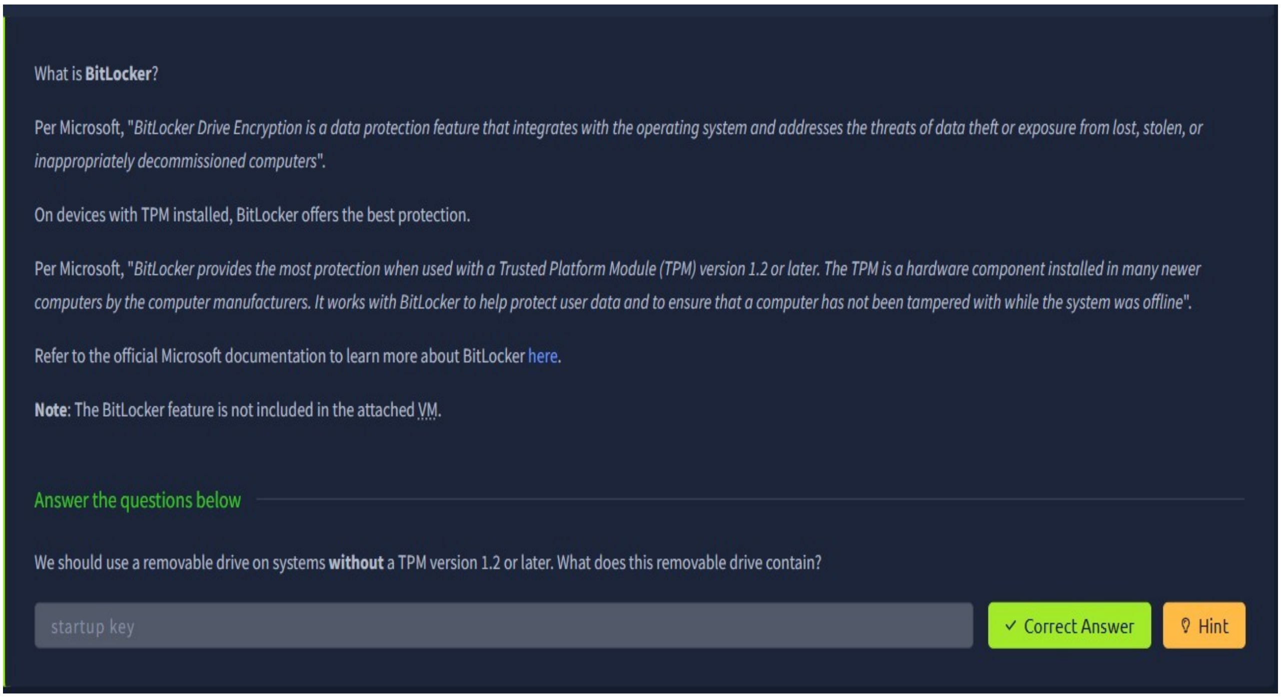
Volume	Next Run Time	Shares	Used
\\?\Vol...	Disabled	0	
C:\	Disabled	1	

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

Answer the questions below

What is VSS?

Volume Shadow Copy Service



What is **BitLocker**?

Per Microsoft, "*BitLocker Drive Encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers*".

On devices with TPM installed, BitLocker offers the best protection.

Per Microsoft, "*BitLocker provides the most protection when used with a Trusted Platform Module (TPM) version 1.2 or later. The TPM is a hardware component installed in many newer computers by the computer manufacturers. It works with BitLocker to help protect user data and to ensure that a computer has not been tampered with while the system was offline*".

Refer to the official Microsoft documentation to learn more about BitLocker here.

Note: The BitLocker feature is not included in the attached VM.

Answer the questions below

We should use a removable drive on systems **without** a TPM version 1.2 or later. What does this removable drive contain?

startup key