Aim of the Experiment:

The **Windows Fundamentals 3** room on TryHackMe focuses on **Windows networking**, including how Windows devices communicate over a network, network configurations, and troubleshooting techniques.

Algorithm for the Experiment:

1. **Check Network Configuration:**
   - Open **Command Prompt** (`cmd.exe`) and run:

     ```
     cmd
     CopyEdit
     ipconfig /all
     ```

   - In **PowerShell**, use:

     ```
     powershell
     CopyEdit
     Get-NetIPAddress
     Get-NetAdapter
     ```

2. **Test Network Connectivity:**
   - Use `ping` to check if a device is reachable:

     ```
     cmd
     CopyEdit
     ping 8.8.8.8
     ```

   - Use `tracert` to track network hops:

     ```
     cmd
     CopyEdit
     tracert google.com
     ```

   - In **PowerShell**:

     ```
     powershell
     CopyEdit
     Test-NetConnection -ComputerName google.com
     ```

3. **View Open Network Connections:**
   - Check active connections:

     ```
     cmd
     CopyEdit
     netstat -ano
     ```

   - View listening ports in **PowerShell**:

     ```
     powershell
     CopyEdit
     Get-NetTCPConnection
     ```

4. **Manage Windows Firewall:**
   - Open **Windows Defender Firewall** (`wf.msc`).
   - View firewall rules in **cmd**:

     ```
     cmd
     CopyEdit
     netsh advfirewall show allprofiles
     ```

   - In **PowerShell**:

     ```
     powershell
     CopyEdit
     Get-NetFirewallRule
     ```

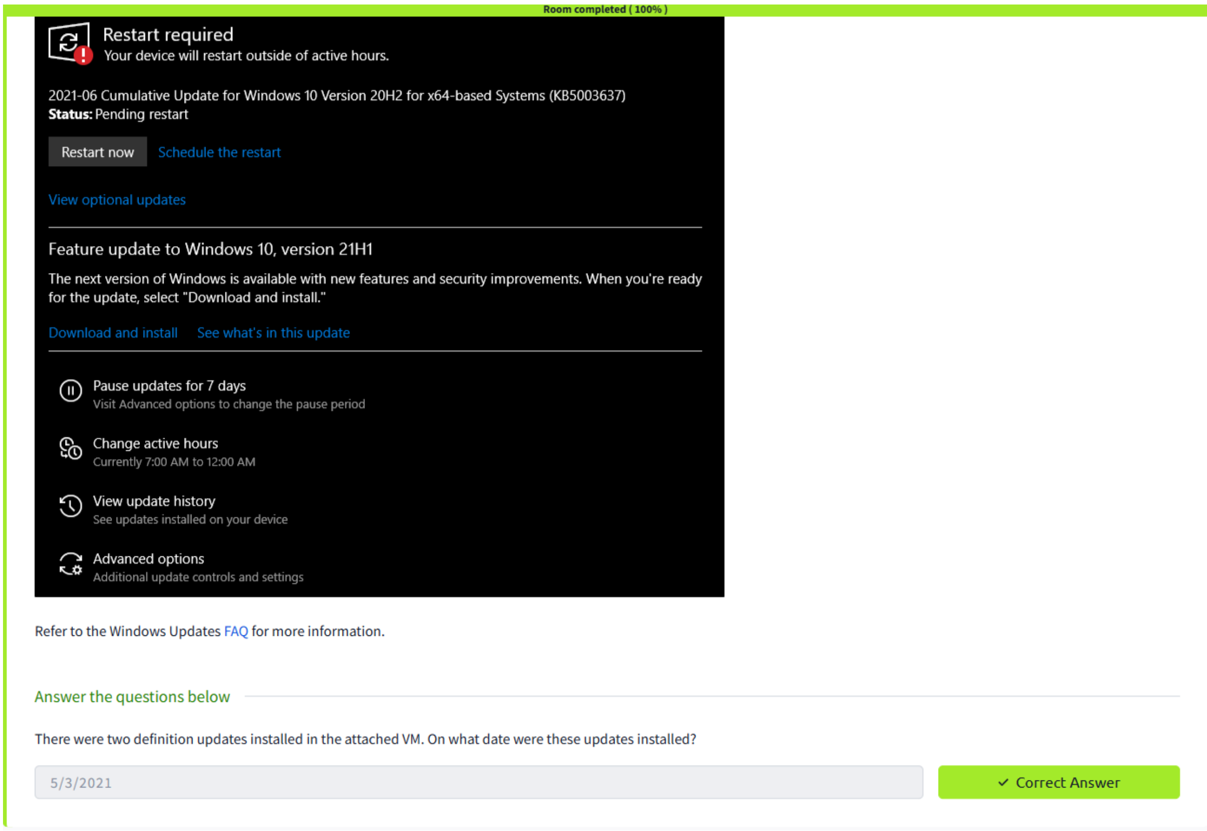
5. **Check Remote Access (RDP & PowerShell Remoting):**
   - Verify if RDP is enabled:

     ```
     powershell
     CopyEdit
     Get-ItemProperty -Path
     'HKLM:\System\CurrentControlSet\Control\Terminal Server' -Name
     fDenyTSConnections
     ```

   - Enable PowerShell Remoting:

     ```
     powershell
     CopyEdit
     Enable-PSRemoting -Force
     ```

6. **Answer TryHackMe Questions:**
   - Use the collected data to complete the TryHackMe room challenges.



Room completed (100%)

Restart required
Your device will restart outside of active hours.

2021-06 Cumulative Update for Windows 10 Version 20H2 for x64-based Systems (KB5003637)
Status: Pending restart

Restart now Schedule the restart

View optional updates

Feature update to Windows 10, version 21H1

The next version of Windows is available with new features and security improvements. When you're ready for the update, select "Download and install."

Download and install See what's in this update

Pause updates for 7 days
Visit Advanced options to change the pause period

Change active hours
Currently 7:00 AM to 12:00 AM

View update history
See updates installed on your device

Advanced options
Additional update controls and settings

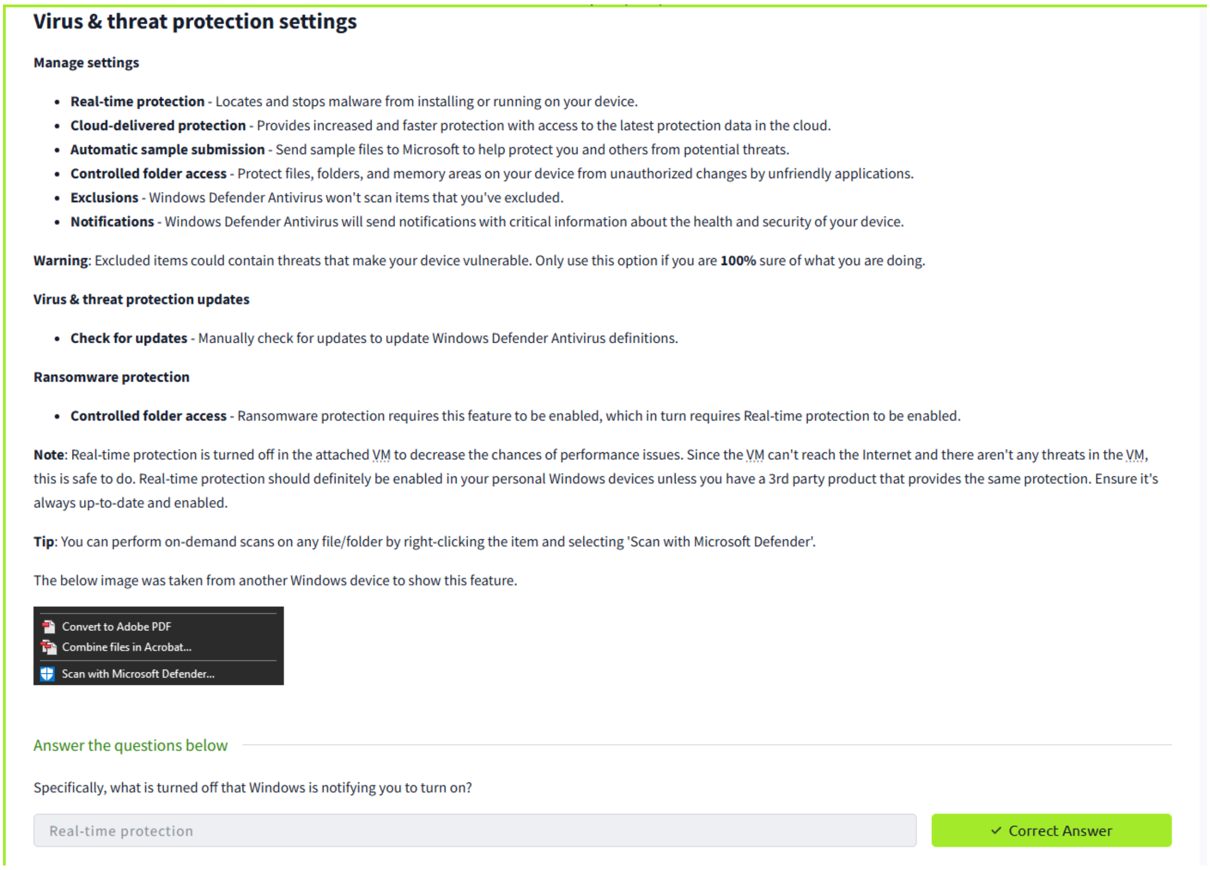
Refer to the Windows Updates FAQ for more information.

Answer the questions below

There were two definition updates installed in the attached VM. On what date were these updates installed?

5/3/2021

✓ Correct Answer



Virus & threat protection settings

Manage settings

- **Real-time protection** - Locates and stops malware from installing or running on your device.
- **Cloud-delivered protection** - Provides increased and faster protection with access to the latest protection data in the cloud.
- **Automatic sample submission** - Send sample files to Microsoft to help protect you and others from potential threats.
- **Controlled folder access** - Protect files, folders, and memory areas on your device from unauthorized changes by unfriendly applications.
- **Exclusions** - Windows Defender Antivirus won't scan items that you've excluded.
- **Notifications** - Windows Defender Antivirus will send notifications with critical information about the health and security of your device.

Warning: Excluded items could contain threats that make your device vulnerable. Only use this option if you are **100%** sure of what you are doing.

Virus & threat protection updates

- **Check for updates** - Manually check for updates to update Windows Defender Antivirus definitions.

Ransomware protection

- **Controlled folder access** - Ransomware protection requires this feature to be enabled, which in turn requires Real-time protection to be enabled.

Note: Real-time protection is turned off in the attached VM to decrease the chances of performance issues. Since the VM can't reach the Internet and there aren't any threats in the VM, this is safe to do. Real-time protection should definitely be enabled in your personal Windows devices unless you have a 3rd party product that provides the same protection. Ensure it's always up-to-date and enabled.

Tip: You can perform on-demand scans on any file/folder by right-clicking the item and selecting 'Scan with Microsoft Defender'.

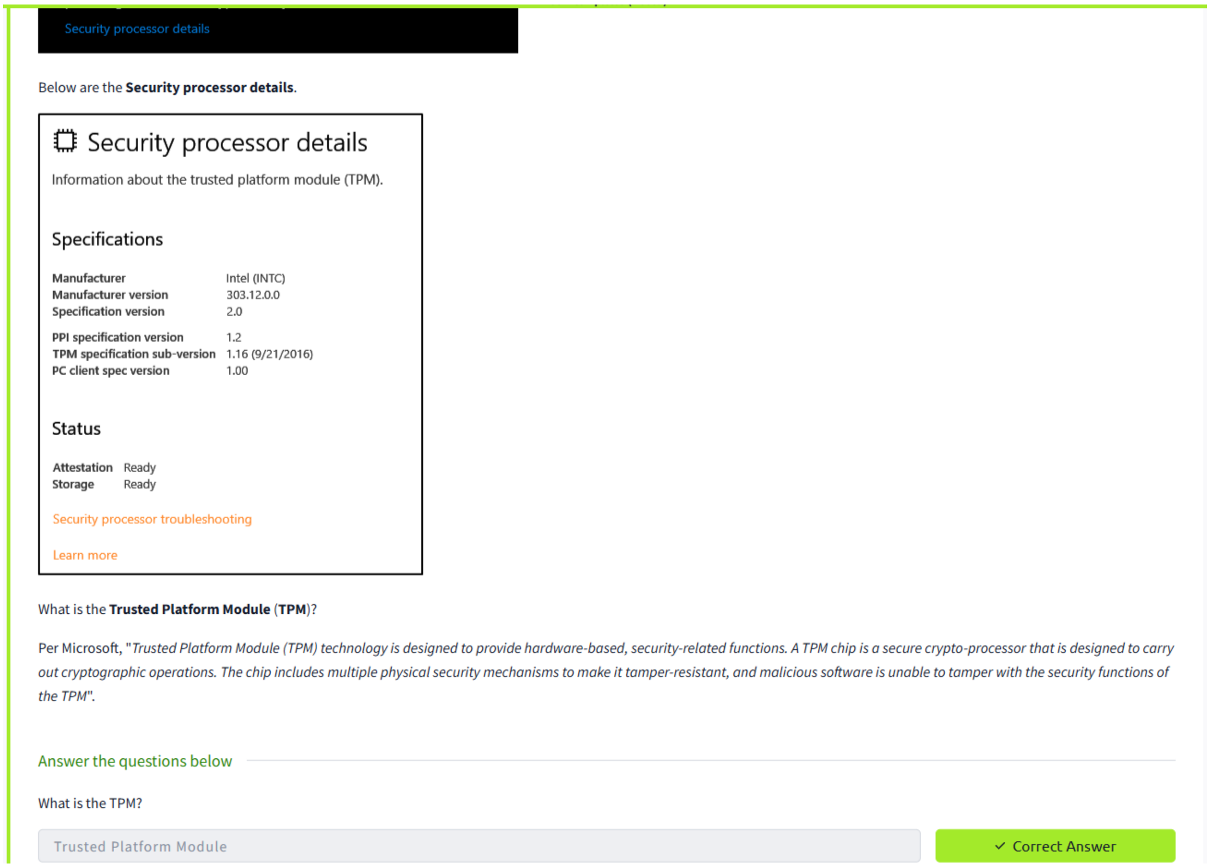
The below image was taken from another Windows device to show this feature.

Answer the questions below

Specifically, what is turned off that Windows is notifying you to turn on?

Real-time protection

✓ Correct Answer



Below are the **Security processor details**.

Security processor details

Information about the trusted platform module (TPM).

Specifications

Manufacturer	Intel (INTC)
Manufacturer version	303.12.0.0
Specification version	2.0
PPI specification version	1.2
TPM specification sub-version	1.16 (9/21/2016)
PC client spec version	1.00

Status

Attestation	Ready
Storage	Ready

Security processor troubleshooting

Learn more

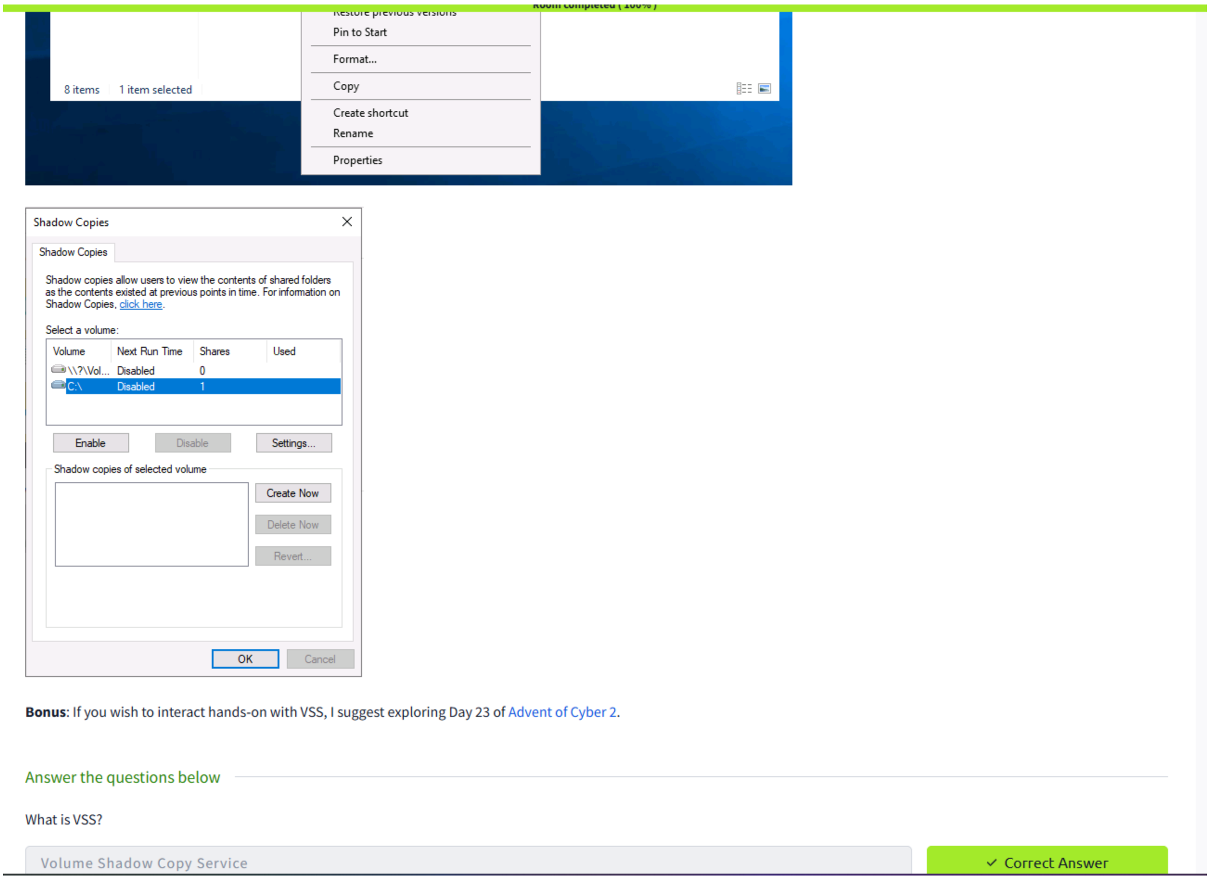
What is the **Trusted Platform Module** (**TPM**)?

Per Microsoft, "*Trusted Platform Module (TPM) technology is designed to provide hardware-based, security-related functions. A TPM chip is a secure crypto-processor that is designed to carry out cryptographic operations. The chip includes multiple physical security mechanisms to make it tamper-resistant, and malicious software is unable to tamper with the security functions of the TPM*".

Answer the questions below

What is the TPM?

Trusted Platform Module



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	

Shadow copies of selected volume

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

✓ Correct Answer