WINDOWS FUNDAMENTALS 3: SECURITY AND SYSTEM PROTECTION

EXP.NO: 1(c)

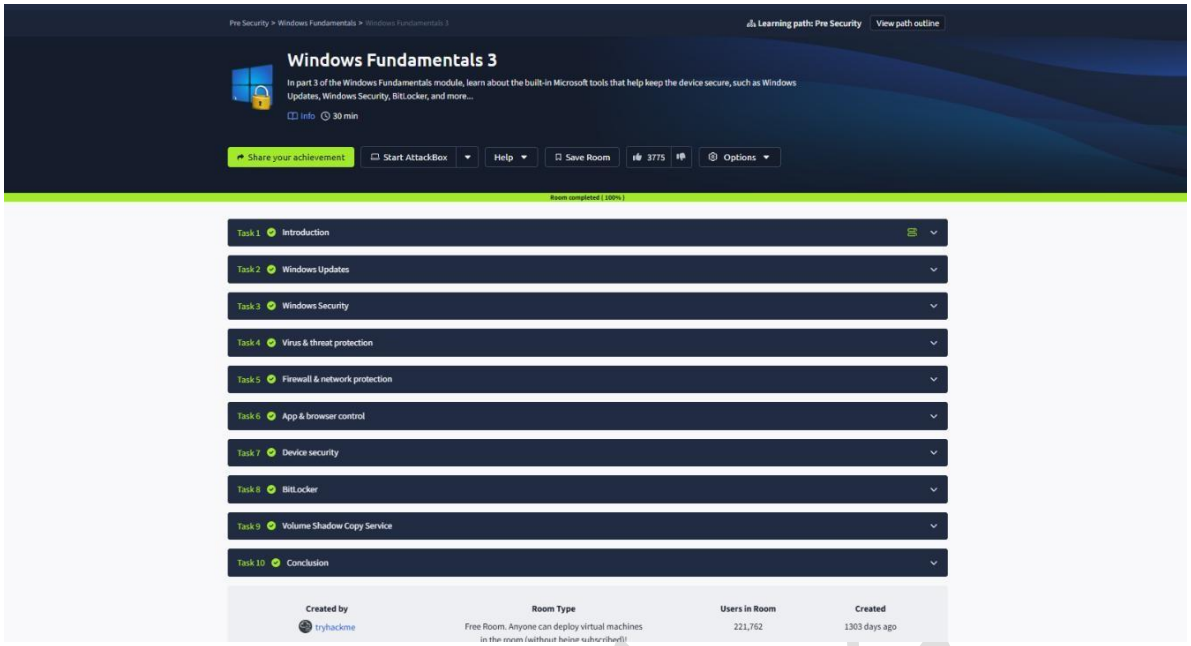
AIM:

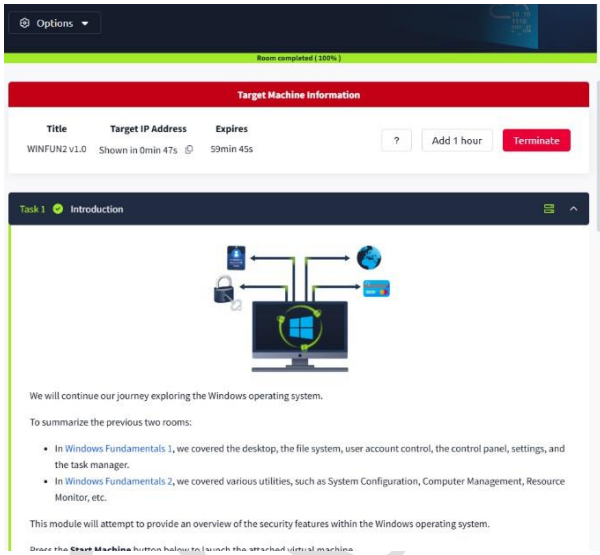
To understand and explore key security features in Windows, including Windows Defender, Firewalls, User Account Control (UAC), BitLocker, and Windows Updates.

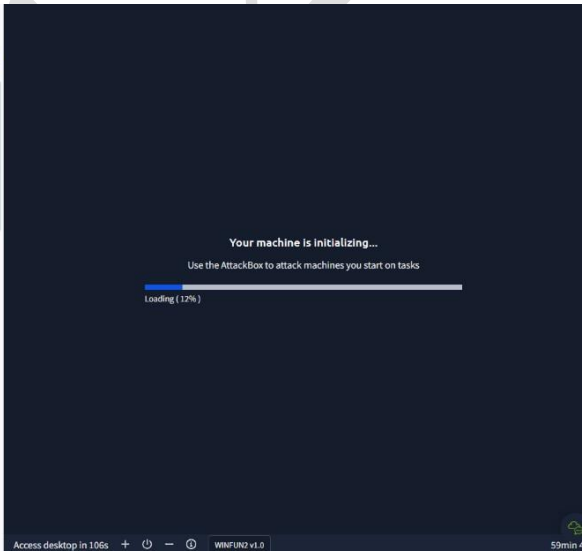
ALGORITHM:

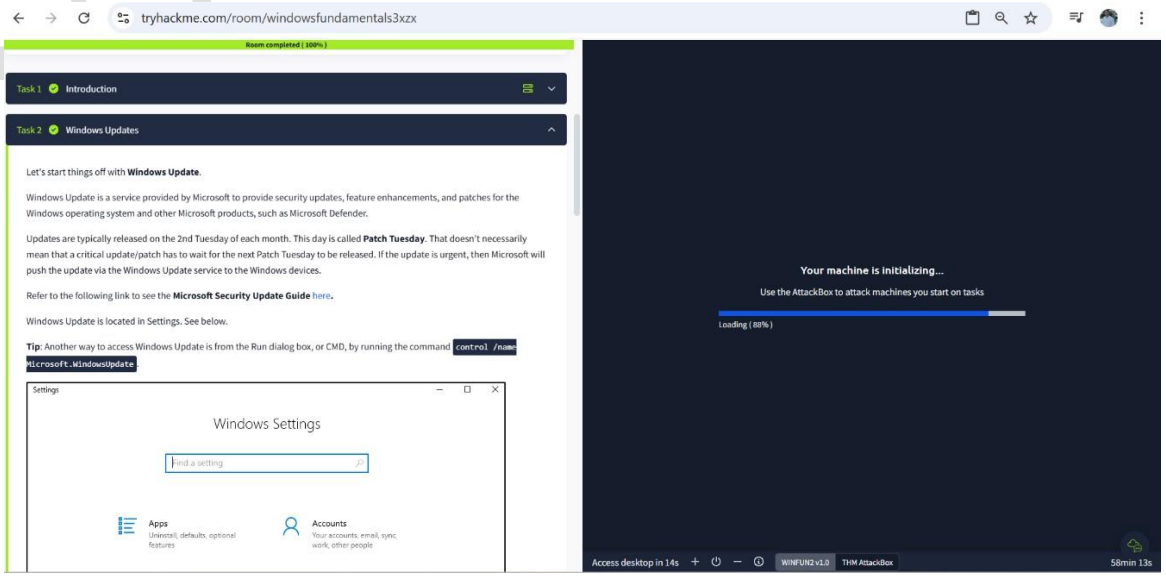
1. Access the lab in TryHackMe platform using the link below https://tryhackme.com/r/room/windowsfundamentalsxzx
2. Click Start a Machine and AttackBox to run the instance of Kali Windows distribution.
3. Solve the task questions start with Windows Update – Patch Tuesday – Windows Setting – Update & Security (or in command prompt type control / name Microsoft.WindowsUpdate .
4. Explore Windows Security → Protection areas, Virus & threat protection, Firewall & network protection, App & browser control, Device security.
5. Learn in Firewall & network protection – Domain network , Private network and Public network – Windows Defender Firewall (WF.msc)
6. Understand the Microsoft Defender SmartScreen – Exploit Protection – System Settings - Program Settings.
7. Explore about Device Security → Core isolation → Memory Integrity , Security Processor → Trusted Platform Module (TPM).
8. Understand about BitLocker – Practical Application – BitLocker and TPM – System Requirements – Device Encryption – TPM versions.
9. Explore Volume Shadow copy Service (VSS) – Advanced System Settings – Create a restore point – Perform system restore – Configure restore settings – Delete restore points.

OUTPUT:


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...
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
Task 8 BitLocker
Task 9 Volume Shadow Copy Service
Task 10 Conclusion
Created by
Room Type
Users in Room
Created
tryhackme
221,762
1303 days ago


Options
Target Machine Information
Title
Target IP Address
Expires
WINFUN2 v1.0
59min 45s
Add 1 hour
Terminate
Task 1 Introduction
We will continue our journey exploring the Windows operating system.
To summarize the previous two rooms:
In Windows Fundamentals 1, we covered the desktop, the file system, user account control, the control panel, settings, and the task manager.
In Windows Fundamentals 2, we covered various utilities, such as System Configuration, Computer Management, Resource Monitor, etc.
This module will attempt to provide an overview of the security features within the Windows operating system.


Your machine is initializing...
Use the AttackBox to attack machines you start on tasks
Loading (12%)
Access desktop in 106s
WINFUN2 v1.0


tryhackme.com/room/windowsfundamentals3xzx
Task 1 Introduction
Task 2 Windows Updates
Let's start things off with Windows Update.
Windows Update is a service provided by Microsoft to provide security updates, feature enhancements, and patches for the Windows operating system and other Microsoft products, such as Microsoft Defender.
Updates are typically released on the 2nd Tuesday of each month. This day is called Patch Tuesday. That doesn't necessarily mean that a critical update/patch has to wait for the next Patch Tuesday to be released. If the update is urgent, then Microsoft will push the update via the Windows Update service to the Windows devices.
Refer to the following link to see the Microsoft Security Update Guide here.
Windows Update is located in Settings. See below.
Tip: Another way to access Windows Update is from the Run dialog box, or CMD, by running the command control /name Microsoft.WindowsUpdate.
Settings
Windows Settings
Find a setting
Apps
Accounts
Your machine is initializing...
Use the AttackBox to attack machines you start on tasks
Loading (88%)
Access desktop in 14s
WINFUN2 v1.0
THM AttackBox
58min 13s

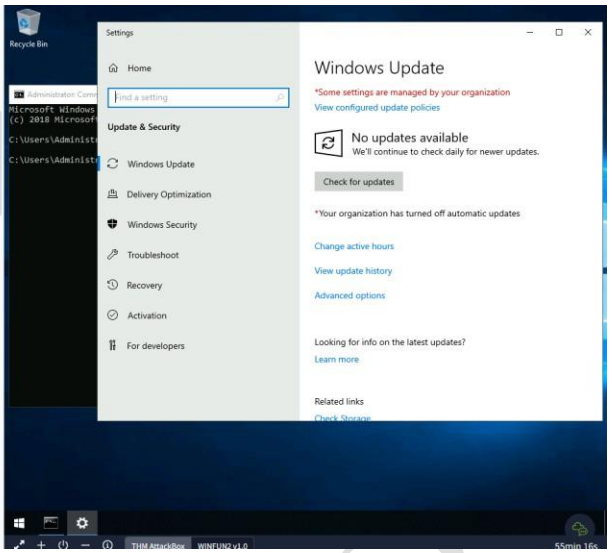
Windows operating system and other Microsoft products, such as Microsoft Defender.

Updates are typically released on the 2nd Tuesday of each month. This day is called **Patch Tuesday**. That doesn't necessarily mean that a critical update/patch has to wait for the next Patch Tuesday to be released. If the update is urgent, then Microsoft will push the update via the Windows Update service to the Windows devices.

Refer to the following link to see the **Microsoft Security Update Guide** here.

Windows Update is located in Settings. See below.

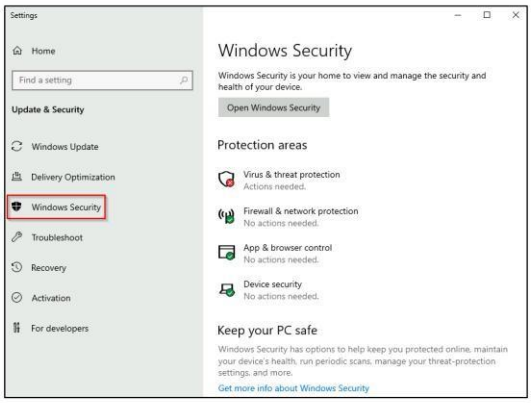
Tip: Another way to access Windows Update is from the Run dialog box, or CMD, by running the command `control /name Microsoft.WindowsUpdate`



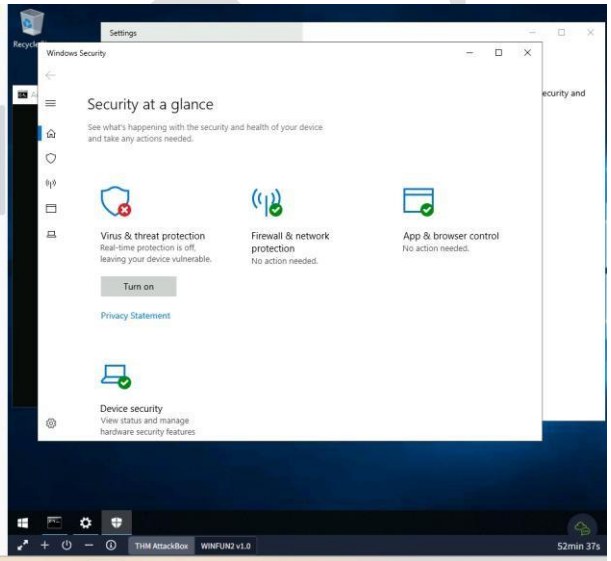
Task 3 Windows Security

Per Microsoft, "***Windows Security*** *is your home to manage the tools that protect your device and your data*".

In case you missed it, **Windows Security** is also available in **Settings**.



In the above image, focus your attention on **Protection areas**.



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.

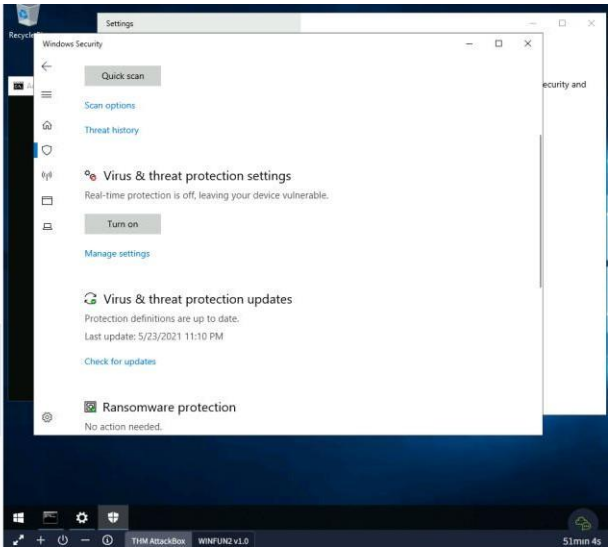
Ransomware protection

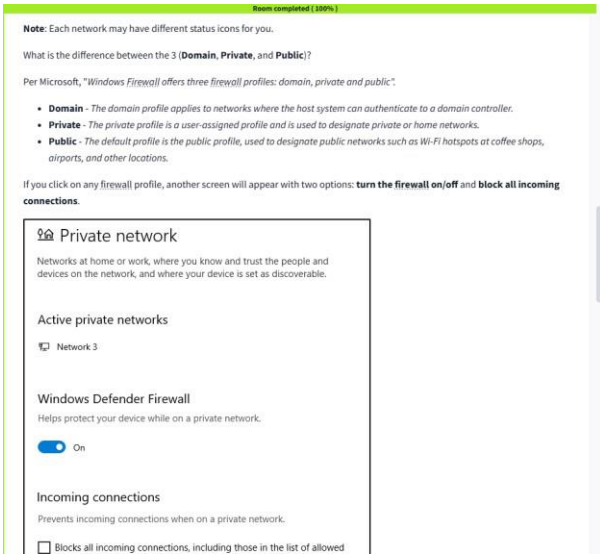
- **Controlled folder access** - Ransomware protection requires this feature to be enabled, which in turn requires Real-time protection to be enabled.

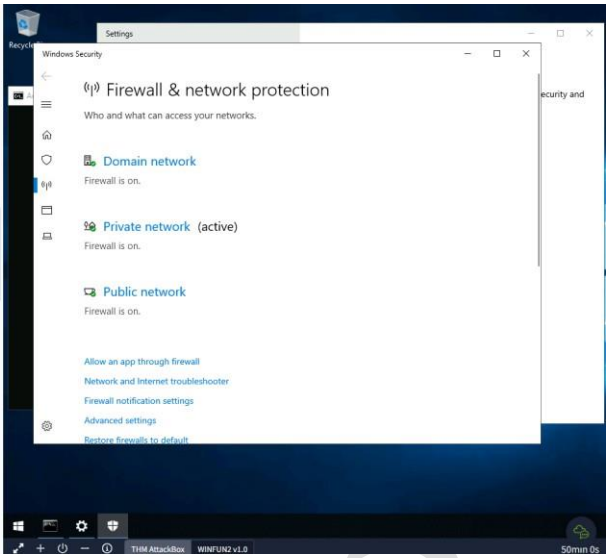
Note: Real-time protection is turned off in the attached VM to decrease the chances of performance issues. Since the VM can't reach the Internet and there aren't any threats in the VM, this is safe to do. Real-time protection should definitely be enabled in your personal Windows devices unless you have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

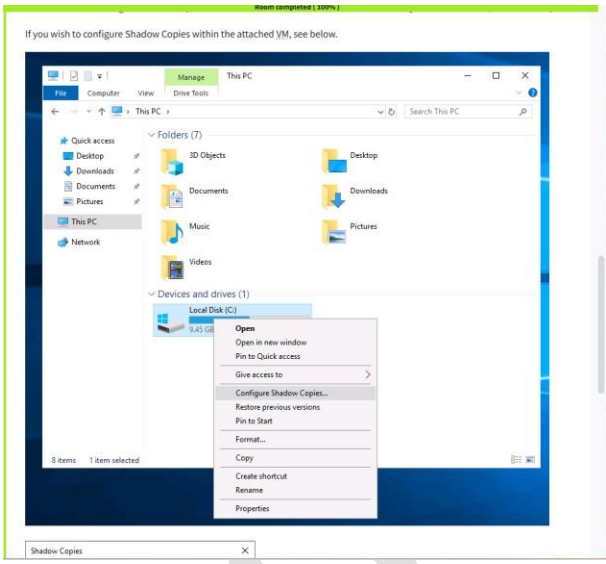
Tip: You can perform on-demand scans on any file/folder by right-clicking the item and selecting 'Scan with Microsoft Defender'.

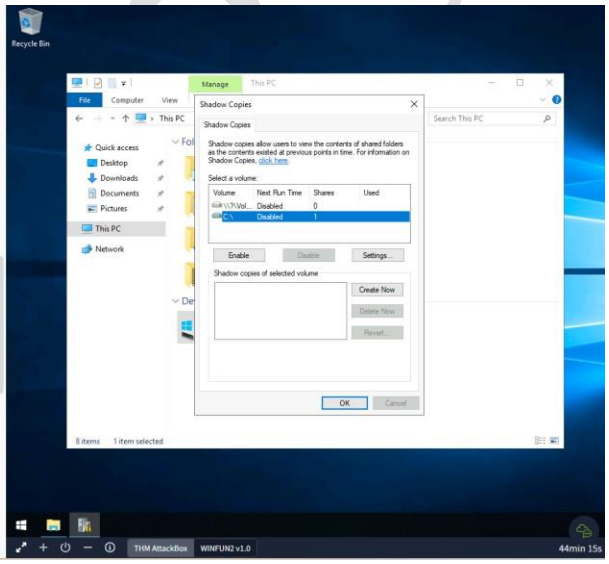
The below image was taken from another Windows device to show this feature.











1. **Windows Defender**
   - Learn about Microsoft's built-in antivirus solution.
   - Understand real-time protection, malware scanning, and threat detection.
   - Explore different scanning options and how Defender integrates with Windows Security.
2. **Windows Firewall**
   - Understand how firewalls protect against unauthorized network traffic.
   - Learn how to configure firewall rules for applications and ports.
   - Explore inbound and outbound connection management

3. **User Account Control (UAC)**
    - Understand the role of UAC in preventing unauthorized changes.
    - Learn how UAC helps restrict administrative privileges to prevent malware execution.
    - Explore different UAC settings and their impact on security.
4. **BitLocker Encryption**
    - Learn how BitLocker encrypts drives to prevent data theft.
    - Explore encryption key management and recovery options.
    - Understand the importance of encrypting removable storage devices.
5. **Windows Updates**
    - Understand the significance of keeping Windows up to date.
    - Learn how updates provide security patches and feature enhancements.
    - Explore how to configure update settings and troubleshoot update issues.

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

Checking the Security section on your VM, which area needs immediate attention?

Virus & threat protection ✓ Correct Answer

If you were connected to airport Wi-Fi, what most likely will be the active firewall profile?

Public network ✓ Correct Answer Hint

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

Real-time protection ✓ Correct Answer

What is the TPM?

Trusted Platform Module ✓ Correct Answer

What is VSS?

Volume Shadow Copy Service ✓ Correct Answer

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

startup key ✓ Correct Answer Hint

RESULT:

This experiment provides an understanding of Windows security best practices and hands-on experience configuring and managing security settings, which is essential for protecting systems from cyber threats.