# **NWIT 246 Hands-on Lab**

**Lab-5b: Harden Windows System to Reduce Attack Surface Area**

**Assignment:**

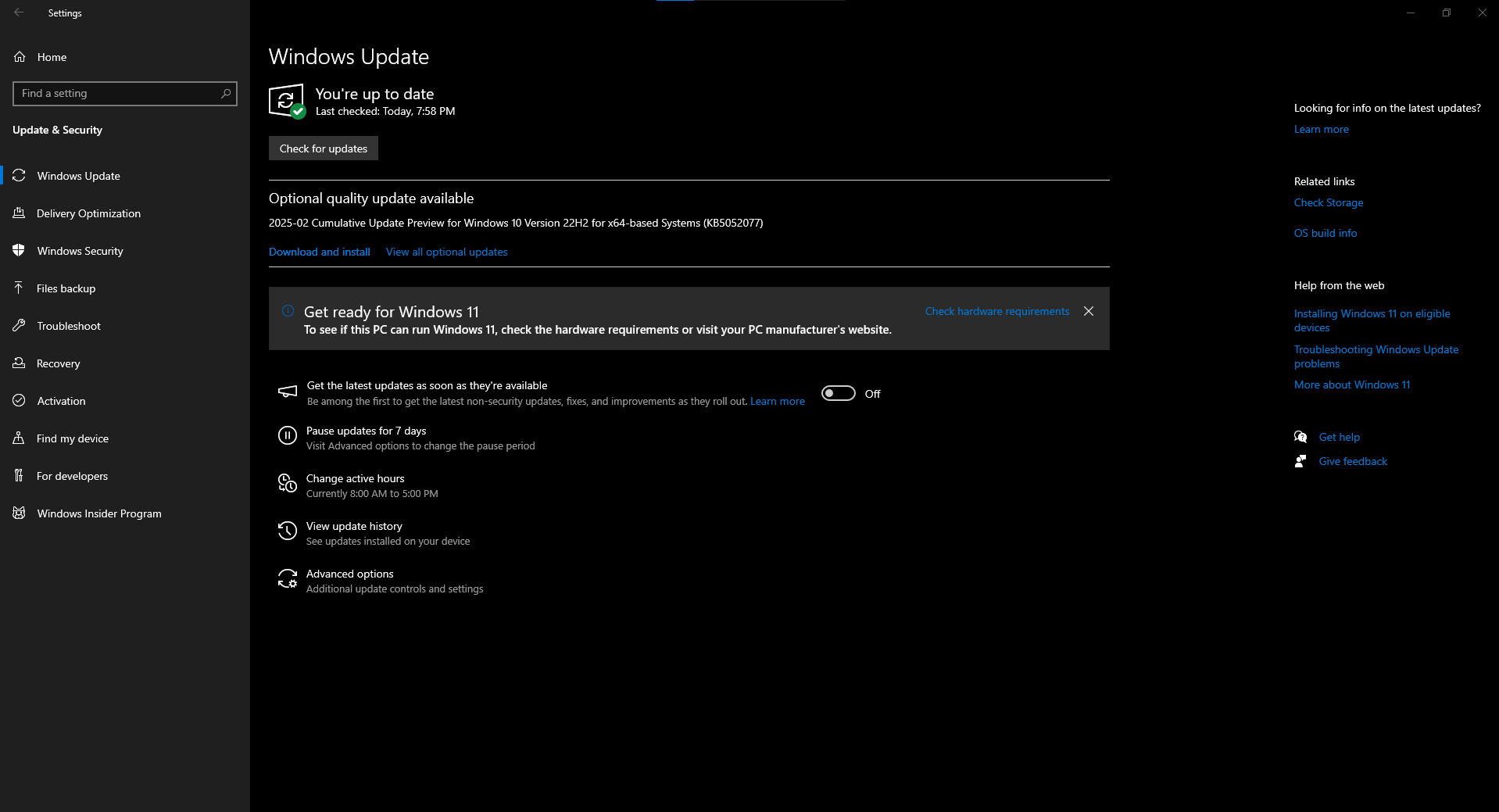
1. OS Updates

Updating Operating systems ensure that your Windows System is up to date with the latest security patches and updates.

They may include Service Packs and Patches.

* Service Packs:- keep programs up to date and install the latest version. No single action can protect against all attacks, especially against a zero-day attack, but using service packs dramatically reduces these risks.
* Patch Management:- includes planning, testing, timely implementation, and continuous auditing, to ensure that OSes and individual programs on client computers are always patched with the latest updates.

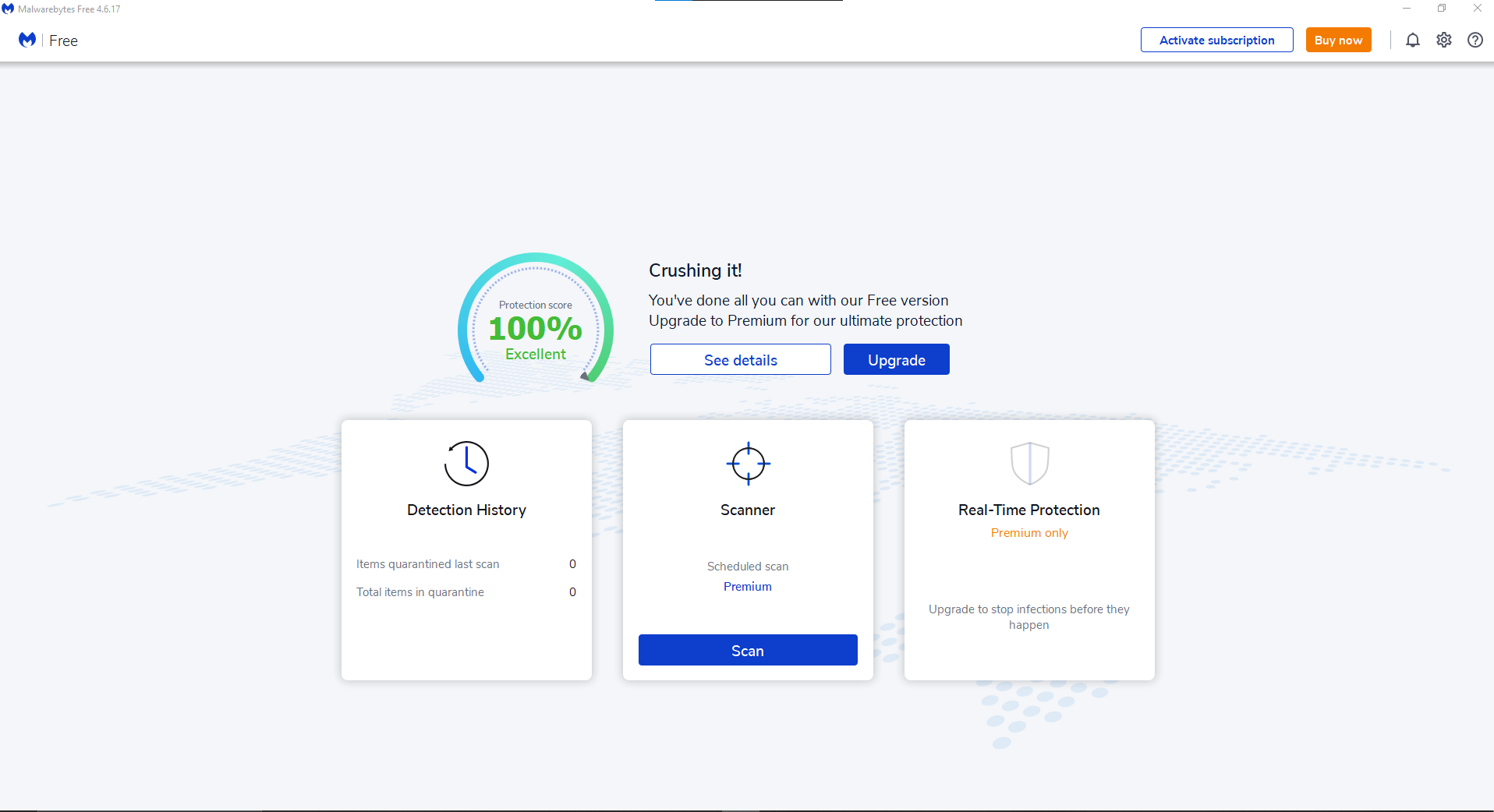
NOTE: For this task, 2 Screenshots are required for “Before and After” the update. So, before you perform the following steps, make sure you take a screenshot for the “Before” screenshots.

1. Open Settings from the Start menu.
2. Once in the Settings window, select “Updates & Security.”
3. Click on “Check for updates”.
4. Take a screenshot of the update and put it next to the “Before” screenshot and label it “After update”. If your system is up to date, make sure to state so and add your **single or two screenshot(s) below.**   
   

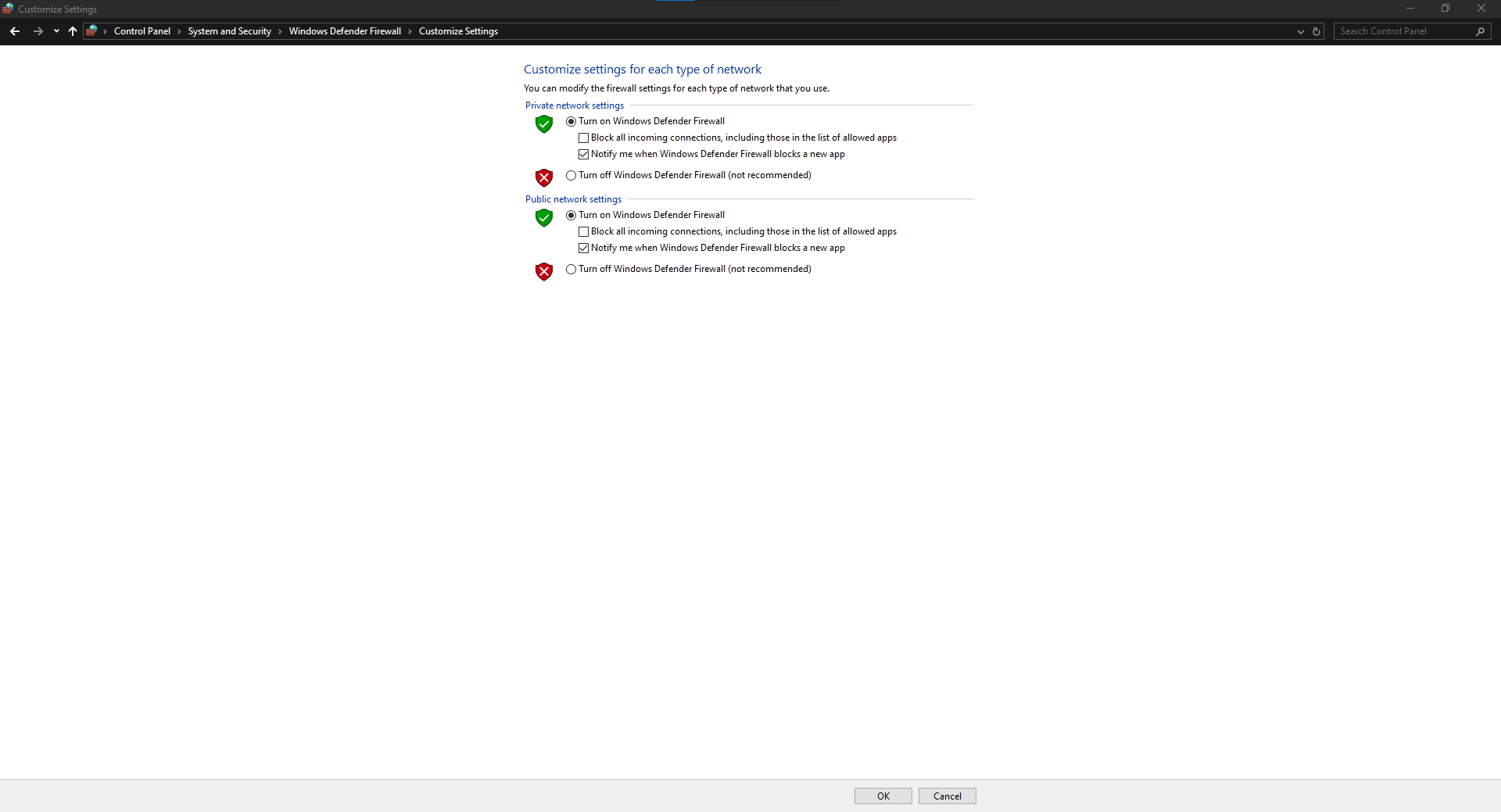
***Windows is up to date***

1. Use Antivirus Software: - Using a reliable Antivirus from a reputable vendor to protect your system from malware and other malicious threats is essential.

* Show an existing Antivirus such as Windows Defender, McAfee, etc. If not, install any well-known version Avs such as Avast, Bitdefender, etc.
* Make sure to research the AV first, then download the software from the vendor site. Then, properly configure the antivirus software.
* Paste your existing or the newly configured AV screenshot below.

  
***Malwarebytes installed on my computer.***

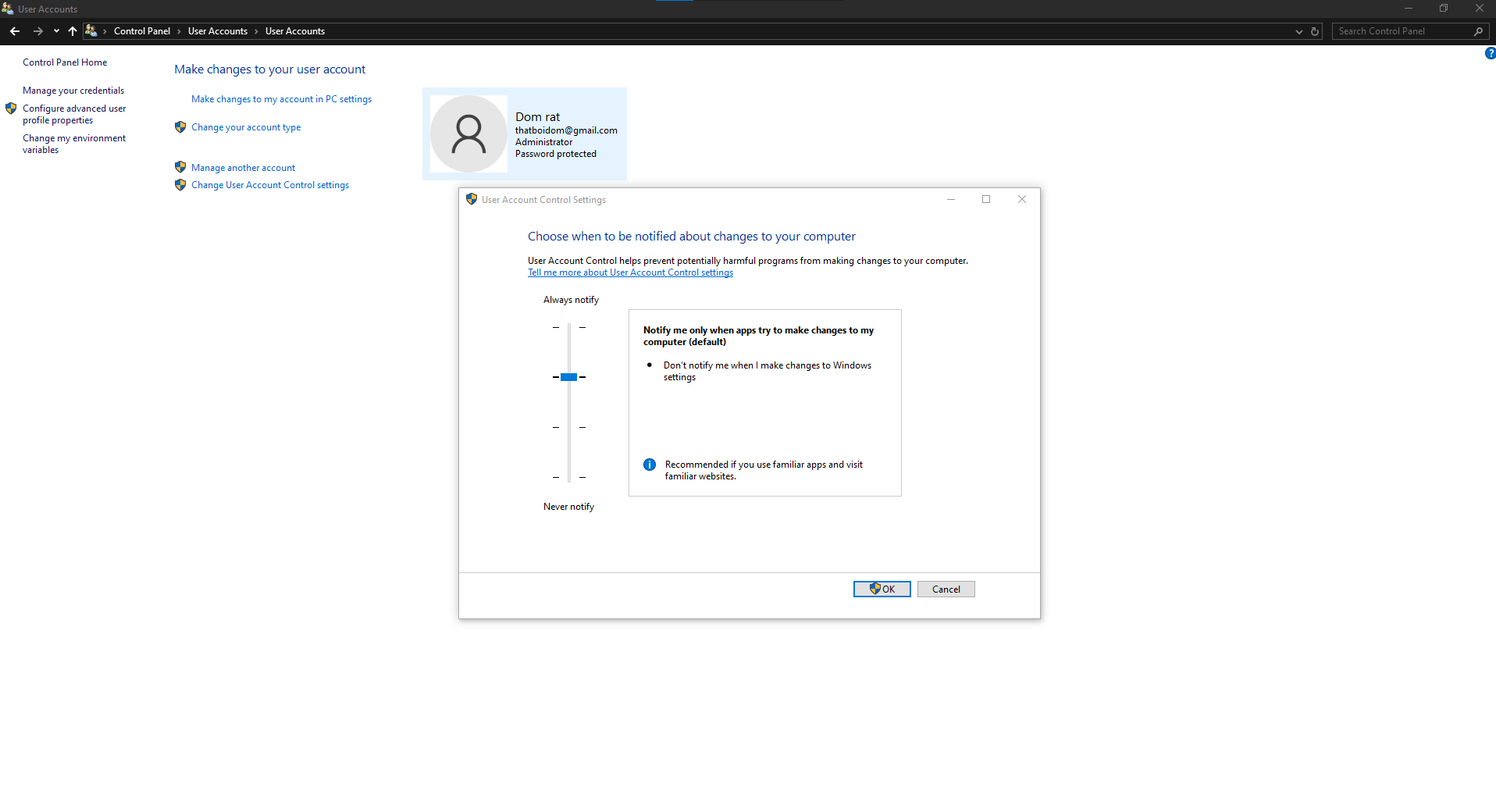
1. Enable Windows Firewall:- Windows Defender Firewall helps prevent hackers and malicious software from gaining access to your PC through the internet or a network. Your organization will require you to turn it on before you can access their network resources from your device.
   1. Open the "Control Panel".
   2. In the Control Panel window, click on "System and Security."
   3. Click on "Windows Defender Firewall."
   4. In the left sidebar, click on "Turn Windows Defender Firewall on or off."
   5. Enable the firewall for both private and public networks.
   6. Capture a screenshot of this setup and paste it below.

  
***Configured firewall***

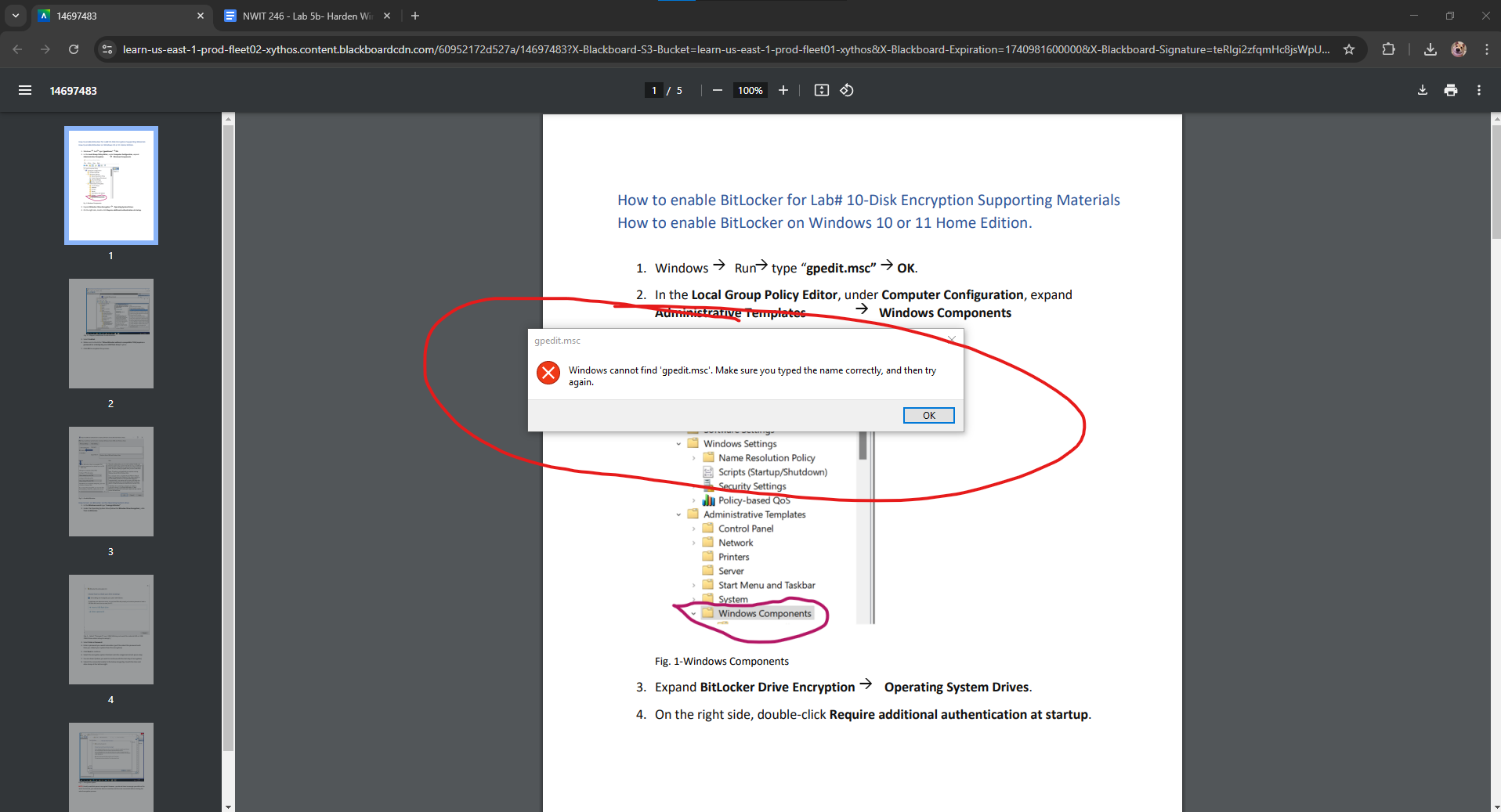
1. Configure User Account Control (UAC): - UAC helps prevent unauthorized changes to your system. When changes to the system require administrator-level permission, UAC notifies the user, giving the opportunity to approve or deny the change. UAC improves the security of Windows devices by limiting the access that malicious code must execute with administrator privileges.

Adjust your UAC settings using the following steps:

* 1. Open "Control Panel."
  2. Click on "User Accounts." X2 (Control Panel\User Accounts\User Accounts)
  3. Select "Change User Account Control settings."
  4. Move the slider to the level of protection you desire (recommended: Default or Always notify).
  5. Click "OK" to save the changes.
  6. Capture a screenshot of this setup and paste it below. (Before /after is optional)

  
***UAC settings slider set to the default level***

1. Enable BitLocker: - If your Windows edition supports it (32 Bit Home Editions are not supported), consider using BitLocker to encrypt your system drive. This step helps protect your data in case of theft or unauthorized access. Here's how to enable BitLocker:
   1. Open the "Control Panel."
   2. Click on "System and Security."
   3. Select "BitLocker Drive Encryption."
   4. Click on "Turn on BitLocker" for your system drive.
   5. Follow the on-screen instructions to set up a strong password or encryption key.
   6. Capture a screenshot of this setup and paste it below. (Before /after is optional)
   7. If your BitLocker is already enabled and/or managed by Sys Admin, consider creating a removable USB-based BitLocker (BitLocker To Go). Very useful and handy.

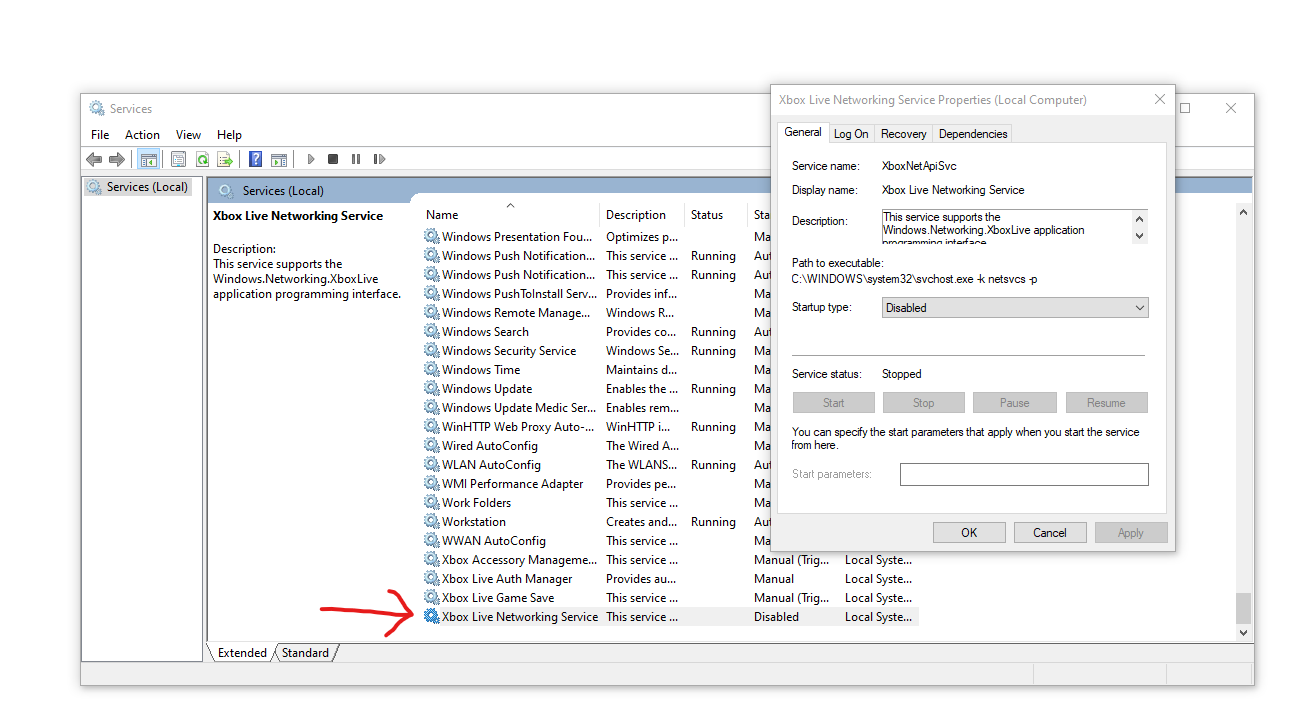


***Unfortunately I have Windows 10 Home edition which means I do not have Bitlocker nor the Local Group Policy Editor, so I am unable to complete this step.***

1. Disable Unnecessary Services or Ports: - You may use these processes based on the document provided a couple of weeks ago in the Announcement section under the name of “To those who haven’t done… no submission required”. The intro, the details as well as the steps that I wrote are much more detailed.

However, if you are interested in shortcuts, you may follow these steps:

* 1. Type "Turn Windows features on or off." On your Windows Search.
  2. Uncheck the features you don't need and click "OK" to save the changes.
  3. To disable services, press Win + R, type "services.msc," and press Enter.
  4. Locate unnecessary services, right-click on them, and choose "Properties."
  5. Set the start/stop/Pause/Resume options to "Disabled/Enable" or "Manual."
  6. Please provide a single screenshot shat shows you disabled a port or a service.

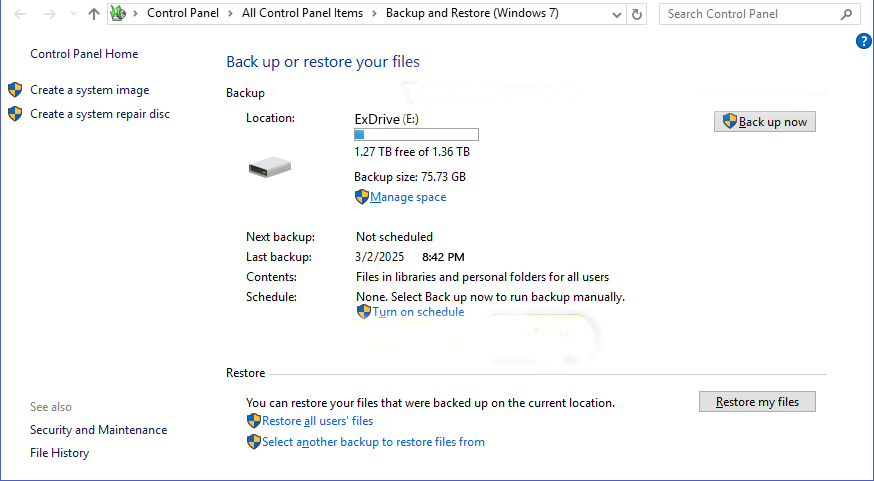
  
***I disabled “Xbox Live Networking Service” as there is no task I would perform on my computer that would require this service to be enabled.***

1. Create a Regular or Periodic Backup (Make any type of system backup-Did somebody say Database?)

Create regular or periodic (on DBMS only) backups of your important data to protect against data loss caused by malware (especially Ransomware), system failures.

Here are the steps to set up a backup:

* + 1. Connect an external storage device to your computer (e.g., USB drive, external hard drive).
    2. Open the "Control Panel."
    3. Click on "System and Security."
    4. Select "Backup and Restore (Windows 7)" or "Backup and Restore."
    5. Click on "Set up backup" and follow the on-screen instructions to configure the backup settings.
    6. Attach a screenshot showing a complete backup configuration.



***Complete backup of external drive***

The below items are optional!

1. Remove unused or legacy applications.
2. Install Host-based Intrusion Detection System:- Consider installing a Host-Based Intrusion Detection System (HIDS) tool to monitor your system for potential security breaches.

Follow these steps to install and configure a HIDS:

* 1. Research and choose a reliable HIDS tool like OSSEC, Tripwire, or Security Onion.
  2. Download the tool from the official website and run the installer.
  3. Follow the on-screen instructions to complete the installation.
  4. Configure the HIDS tool according to your requirements and enable real-time monitoring.

You are done!