Lab Setup

Virtual Machine

You will need a virtual machine (VM) setup with Windows 10/11 64-bit. If you **do not** already have this setup you can use Virtual Box and a free copy of Windows 10 to get started.

- https://www.virtualbox.org/
- https://www.microsoft.com/en-us/software-download/windows10ISO

If you have an **M1/M2 MacBook**, you will need to follow a special setup running an ARM version of Windows. We strongly recommend using VMWare Fusion and following the guide.

- https://communities.vmware.com/t5/VMware-Fusion-Documents/The-Unofficial-Fusion-13-for-Apple-Silicon-Companion-Guide/ta-p/2939907

Disable Windows Defender

Make sure to disable Windows Defender prior to copying the Lab data to your VM.

- Disabling Tamper Protection
  - https://support.microsoft.com/en-us/windows/prevent-changes-to-security-settings-with-tamper-protection-31d51aaa-645d-408e-6ce7-8d7f8e593f87
  - https://www.tenforums.com/tutorials/123792-turn-off-tamper-protection-windows-defender-antivirus.html

- Disabling Windows Defender
  - https://stackoverflow.com/questions/62174426/how-to-permanently-disable-windows-defender-real-time-protection-with-gpo
  - https://www.windowscentral.com/how-permanently-disable-windows-defender-windows-10
  - https://github.com/jeremybeaume/tools/blob/master/disable-defender.ps1

Required Software

The following software is required to complete the labs.

- IDA Free
  - https://hex-rays.com/ida-free/
- x64dbg
  - https://x64dbg.com/
- IDE of your choice (pick one)
  - https://www.sublimetext.com/
  - https://code.visualstudio.com/

Python Environment

To set up your Python development environment, you will need to install the following.

- Install Python >= 3.9.5
  - https://www.python.org/downloads/

- https://www.python.org/downloads/release/python-395/

- Install Python modules using pip

```
pip install -r requirements.txt
```

Jupyter Lab Test

Test your python environment by running the following from your command prompt. This should open a new Jupyter Notebook in your browser.

```
jupyter-lab
```