Training Prerequisite & Lab Setup Guide

This training consists of two parts*: malware analysis* and *memory forensics*. The malware analysis involves analyzing the malware samples in an isolated virtualized environment and memory forensics is the analysis of computer's RAM to identify forensic artifacts.

Since this is a hands-on training, the students attending the training are required to read this document carefully and make sure the below requirements are met before attending the training. This is to ensure that students have the required lab environment to perform lab exercises.

1) Hardware Pre-requisites

Minimum hardware requirements are as follows:

- 2.0 GHZ CPU and 6GB of RAM (more memory the better) – you will be performing processor and memory intensive operations during the lab assignments.
- 40 GB of disk space (more space the better) – you will receive approximately 5GB compressed memory dumps and malware samples for labs. When uncompressed, it can take up close to double that amount of disk space. You will also receive a pre-built Linux VMware image which is approximately 5 GB when uncompressed.
- USB2.0/3.0 ports – the lab files, course materials & lab solution manual will initially be supplied to you via USB sticks, thus you must ensure that you have at least one of these external USB slots available.

2) Mandatory Software Pre-requisites

a) VMware Workstation (for Windows/Linux)/VMware Fusion (for Mac OSX): There are no restrictions on the host operating system (OS) of the laptop that you bring to the class – Host OS can be Windows, Linux or Mac. It is mandatory to have access to the following resources.

- Download and Install *VMware Workstation/Fusion*. VMware Workstation/Fusion can be commercial or trial version (VMware offers 30 day free trial, you can download it if you don't have the commercial version)

  VMware Workstation (For Windows or Linux) Trial version can be downloaded from the below link
  https://www.vmware.com/products/workstation/workstation-evaluation.html

  VMware Fusion (For Mac operating system) Trial version can be downloaded from the below link
  https://www.vmware.com/products/fusion/fusion-evaluation.html

- Please make sure to install a virtualized instance of Windows operating system inside VMware Workstation/ VMware Fusion. You are free to install anything from Windows 7 (64-bit) to Windows 10 (64-bit) versions inside the VM, most malware samples used in this training are tested on Windows 10 but should work on other versions as well. In addition to installing Windows inside VMware, you must also have full Administrator access to the Windows installed inside the VMware.

Note: We do not distribute Windows Operating system due to licensing terms, so its student's responsibility to install Windows operating system inside the Virtual machine. If you wish you can use the free ***Windows 10 x64*** virtual machines (***MSEdge on Win10 x64***) for VMware distributed by Microsoft here: https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/

- Ability to transfer files from your Host OS into your Virtual Machines (this can be achieved by installing VMware tools). Once Windows OS is installed on your Virtual machine make sure to install VMware tools, this can be done by powering on Windows VM and then by clicking on *VM (or Virtual Machine)* tab and by choosing *Install VMware Tools* and then follow the instructions.

Note: *VMware player or VirtualBox is not recommended for this training, as it lacks some of the features required for the training.*

The reason why we ask to do this:

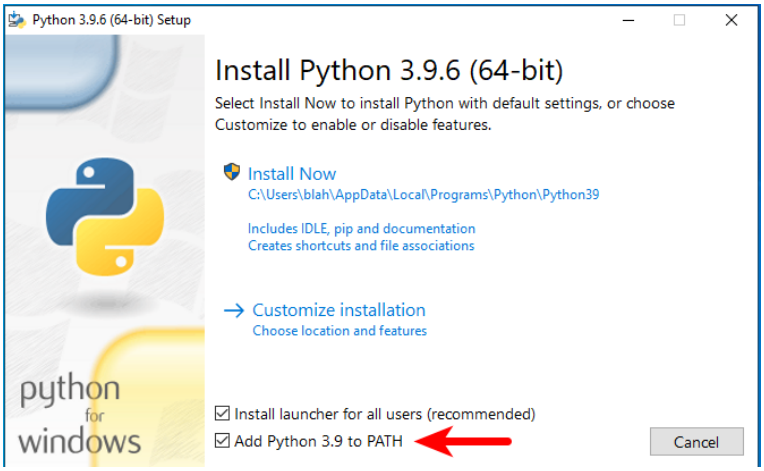
- The reason why we suggest installing Windows in Virtualized environment is because you will be analyzing the real world Windows malware samples by running them in a virtual environment.
- A Linux VM will be provided. You are asked to open the Linux VM in the virtualization software (VMware Workstation or VMware Fusion). This Linux VM contains all the necessary tools pre-installed.
- Most of the labs require you to analyze malware samples or dump malicious content from the memory image; there is a possibility that this malicious content can be deleted by the Antivirus software. Thus it may be best for you to install and run tools within a VM and also make sure that all the security products are disabled on the Windows VM (as the security products can interfere with your analysis)

b) Python 3.x: Some of the analysis tools rely on python. In order to run these tools Python 3.x version is required (not Python 2.x). Download and install the latest 3.x Python on the Windows machine which is installed inside the VMware Workstation/Fusion.

Python Windows installer can be downloaded from the below link:

https://www.python.org

When installing Python, make sure to add Python to the PATH by checking the option shown in the following screenshot.



c) Tools & Softwares:

The attendees are required to install/copy the below mentioned softwares inside Windows VM (running on VMware Workstation/Fusion) before attending the training. The below mentioned tools will be used throughout the training and it would save time if students install these softwares beforehand.

We have bundled all the tools/softwares required for this training into a single zip file, this should save time from downloading all the tools individually. This bundle can be downloaded from the below link:

Download Link: https://www.dropbox.com/s/d3rk513z9lf6r1l/softwares.zip?dl=0

In case you wish to download these tools individually then it can downloaded from the links mentioned below.

Once the tools/softwares are downloaded please make sure that these tools/softwares are copied inside the Windows VM.

- ***IDA Freeware for Windows***: We will be using IDA freeware version to analyze (disassemble and debug) malware sample. It can downloaded from the below link

  https://www.hex-rays.com/products/ida/support/download_freeware/

- ***IDA Demo (Evaluation) Version:*** The evaluation version allows you to explore the latest features of IDA but it has limited functionality (we recommend using IDA Freeware mentioned above, instead of this version). If you have the commercial version of IDA then you are free to use that in the training. If you wish to use the evaluation version of IDA then it can be requested from the below link:

  https://out7.hex-rays.com/demo

- ***X64dbg:*** is an open source 32-bit and 64-bit debugger for Windows. You will also be using this tool for debugging malicious binary. The latest version of x64dbg can be downloaded from the below link:
  https://x64dbg.com/

- ***SysInternals Suite:***
  The sysinternals suite is a set of utilities for system administration, troubleshooting and analysis of windows system. SysInternals suite can be downloaded from
  http://technet.microsoft.com/en-in/sysinternals/bb842062.aspx
  These tools doesn't require any installation, just unzip into the desired folder.

- ***Process Hacker:*** This tool allows you to inspect various process related attributes. You can download either the installer or the portable version from the below link
  http://processhacker.sourceforge.net/downloads.php

- ***CFF Explorer Suite:*** This tool allows you to inspect portable executable (PE) file attributes. This can be downloaded from the below link

http://www.ntcore.com/exsuite.php

- ***Pestudio Free Version:*** This tool allows you to inspect portable executable (PE) file attributes and also allows you to perform malware initial assessment. This tool can be downloaded from the link below.
  https://www.winitor.com/features

- ***Noriben:*** Noriben is a Python-based script that works in conjunction with Sysinternals Procmon to automatically collect, analyze, and report on runtime indicators of malware. Please download and unzip into the desired folder.

  https://github.com/Rurik/Noriben

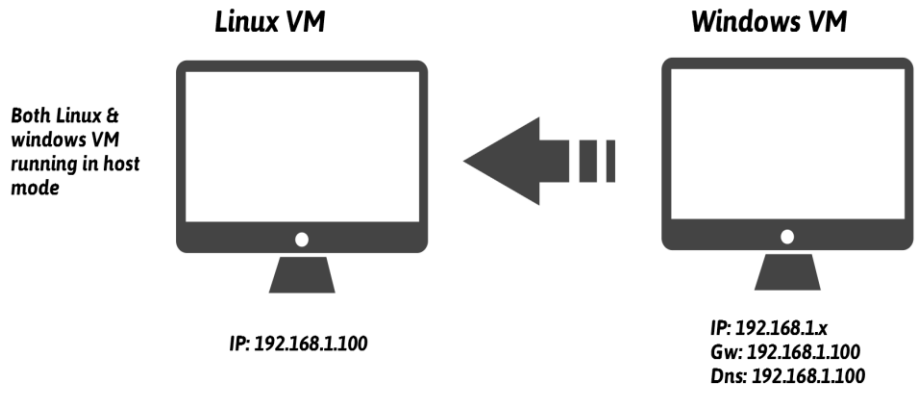
- ***Resource Hacker:*** This program allows you to examine the resources in the Windows executable. It can be downloaded from the following link
  http://www.angusj.com/resourcehacker/

Training Lab Setup Guide

This section contains the details of the lab setup required for the training. Since this is a hands-on training the students attending the training are required to read this section carefully and ***make sure the below requirements are met before attending the training***. This is to ensure that students have the required lab environment to perform lab exercises.

Lab Architecture

The lab setup consists of two virtual machines, one running *Linux VM* (provided by us) and a *Windows Virtual machine* (installed by you on VMware Workstation/fusion). Both Linux VM and Windows VM should be configured to use ***host-only*** *mode*. The IP address of the Linux VM is pre-configured to be ***192.168.1.100*** (please don't change it) and the IP address of Windows VM need to be set to ***192.168.1.x*** *(where x is any number between 1 to 254)*. The *default gateway* and the *DNS server* address on Windows VM should be set to the IP address of the Linux VM (*i.e. 192.168.1.100*) as shown in the below screenshot



1) Setting & Configuring Linux VM

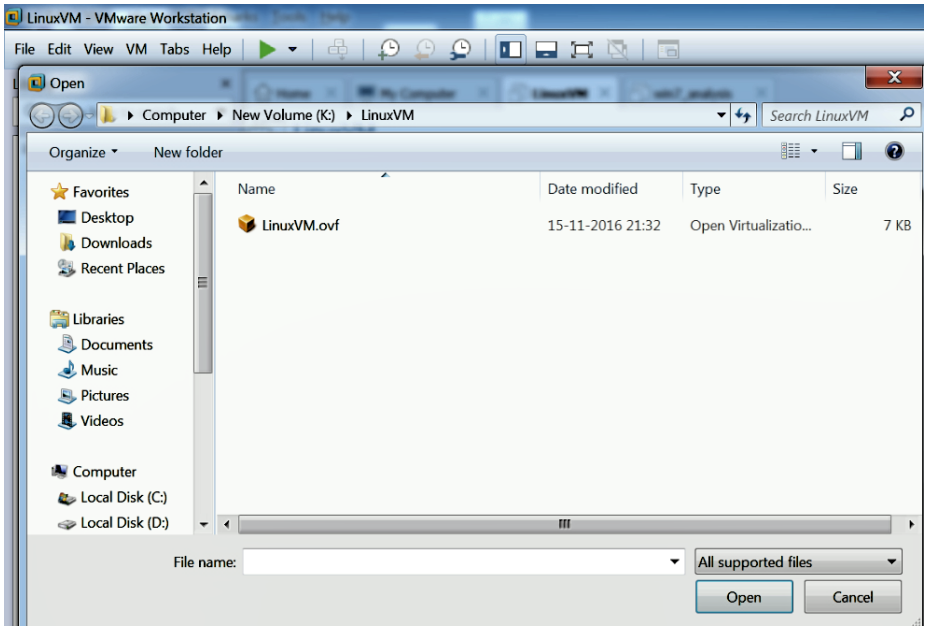
Below is the link to download the zip file containing Linux VM image. Please download and follow the procedure mentioned below

Download Link: https://www.dropbox.com/s/zbhc47xwarcof2x/LinuxVM.zip?dl=0

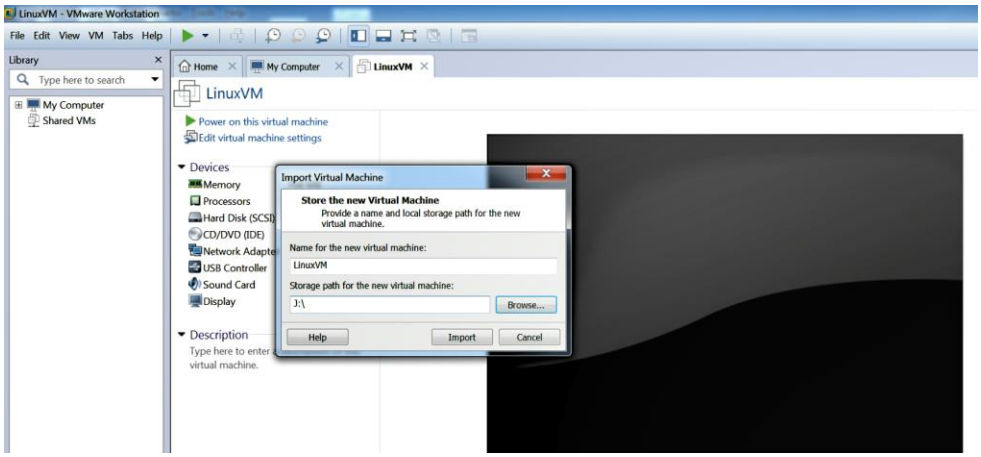
- Unzip the file (***LinuxVM.zip***) to a desired folder.

- Open VMware Workstation, click on ***File -> open*** (or ***File -> import*** *on Mac OS X)* and then navigate to the folder where you have extracted the file containing Linux VM.

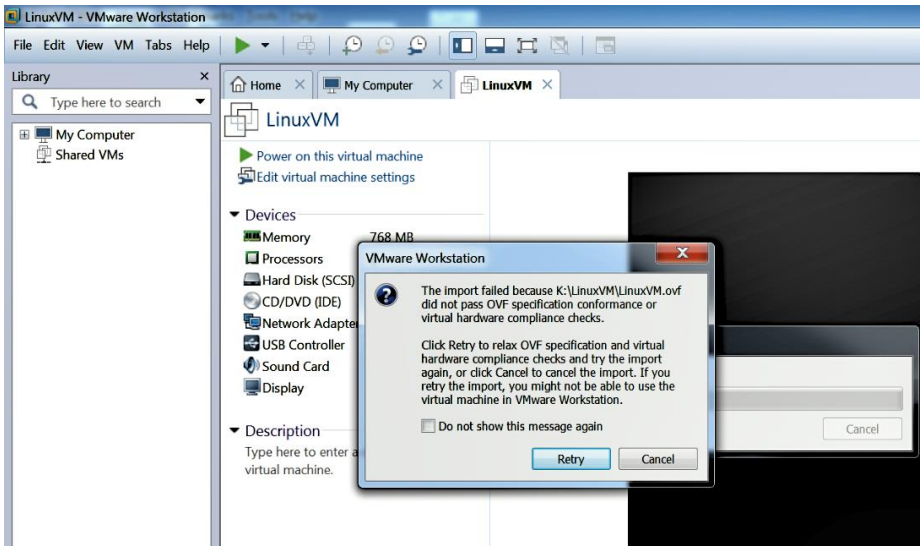
- Select the ***LinuxVM.ovf*** file and click on open as shown in the below screenshot



- Choose the path where your virtual machine needs to installed and click on *import*.

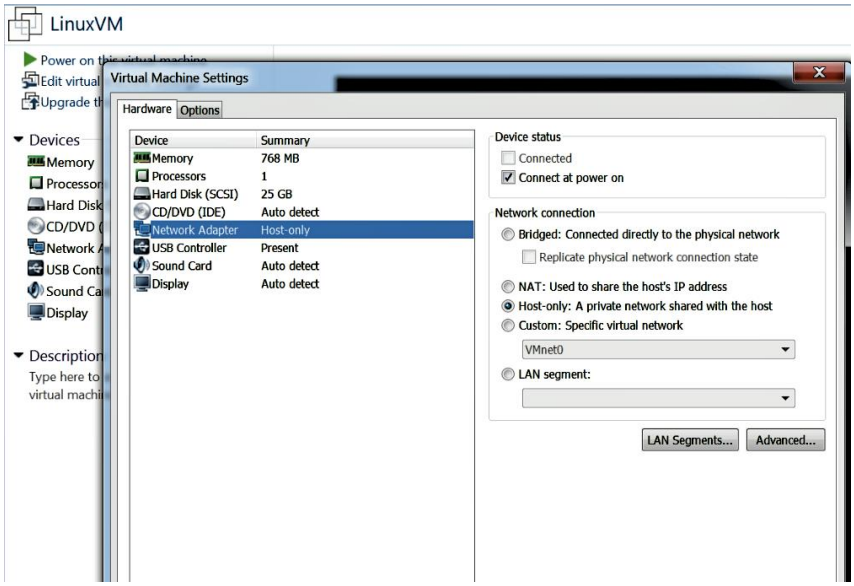


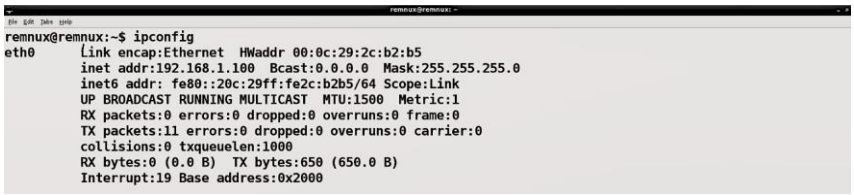
When importing the image, VMware Workstation/Fusion might give a warning prompt as shown below, if you get this prompt just click on *retry*



- Once the import is successful the setup is complete.
- Now you are ready to power on the *Linux VM*.

The IP address of this Linux machine is pre-configured to ***192.168.1.100*** and it is set to run in the host only mode as shown in the below screenshots. Please do not change IP address of the Linux VM because some configuration depends on this IP address.





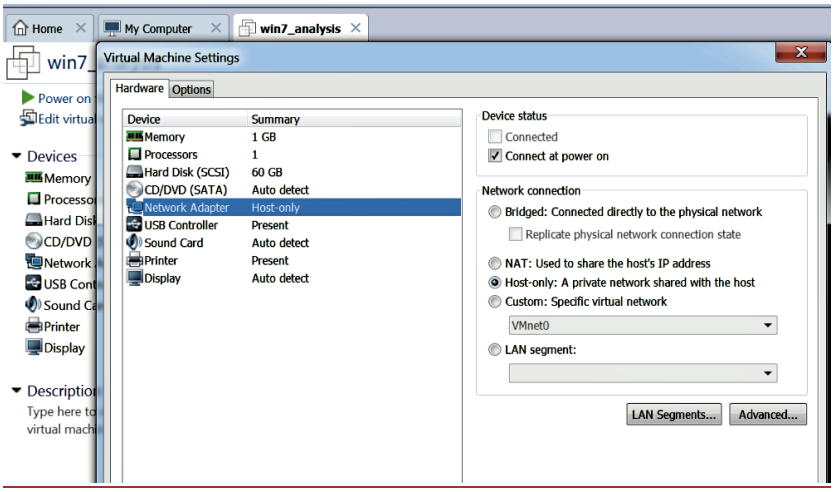
2) Setting & Configuring Windows VM

This section assumes that you have already installed the Windows Operating system in the VMware Workstation/Fusion, and have downloaded and copied the tools & softwares (mentioned earlier in this document) inside the Windows VM.

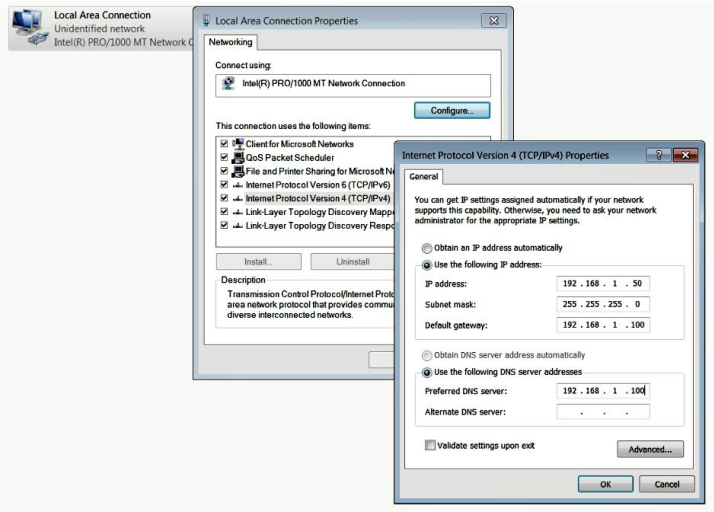
Note: If you are looking for Windows VM then you can get the free ***Windows 10 x64*** virtual machine (***MSEdge on Win10 x64***) for VMware distributed by Microsoft here:

https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/

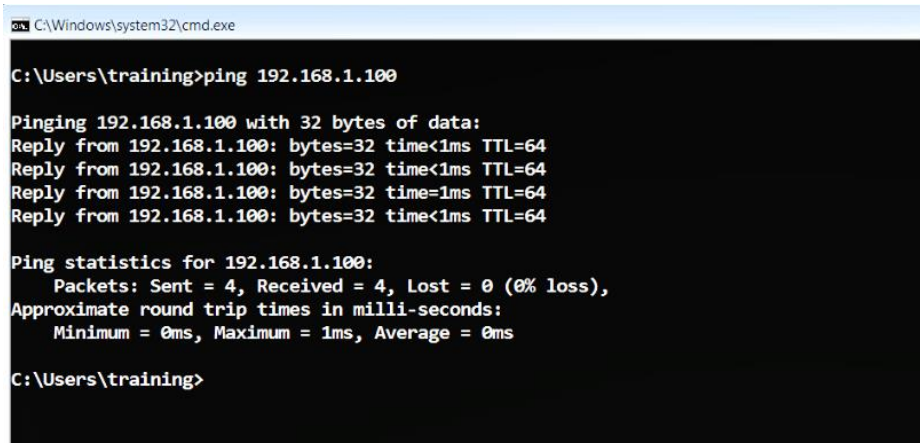
After the Windows operating system is installed in the VMware Workstation/Fusion, Please make sure to configure your Windows VM to run in the ***Host-only*** mode from the Virtual Machine settings as shown below.



Configure the IP address of the *Windows VM* to ***192.168.1.x*** (choose any IP address except ***192.168.1.100*** because the *Linux VM* will be using this IP) and set the *Default gateway* and the *Preferred DNS server* to the IP address of Linux VM (i.e. ***192.168.1.100***) as shown below.



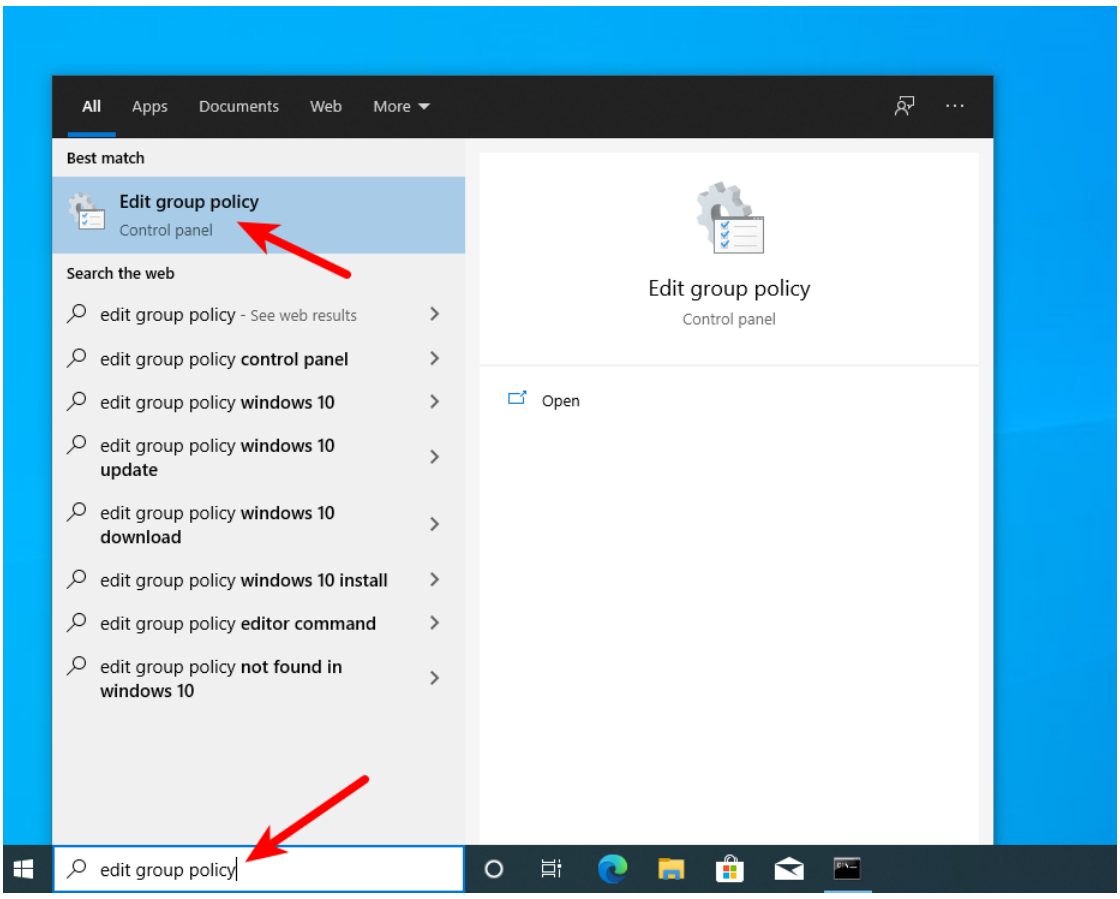
Now power on both the *Linux VM* and *Window VM* and make sure they are able to communicate with each other. You can check for the connectivity by logging into the Windows VM and running the *ping* command as shown below.



After the connectivity between Windows & Linux VM is verified. Please make sure that all the security products are disabled on the *Window VM* as you will be running malware samples on this machine.

Also please disable ***Windows Defender Antivirus (or Windows Defender)*** Service on your Windows VM using the procedure mentioned below:

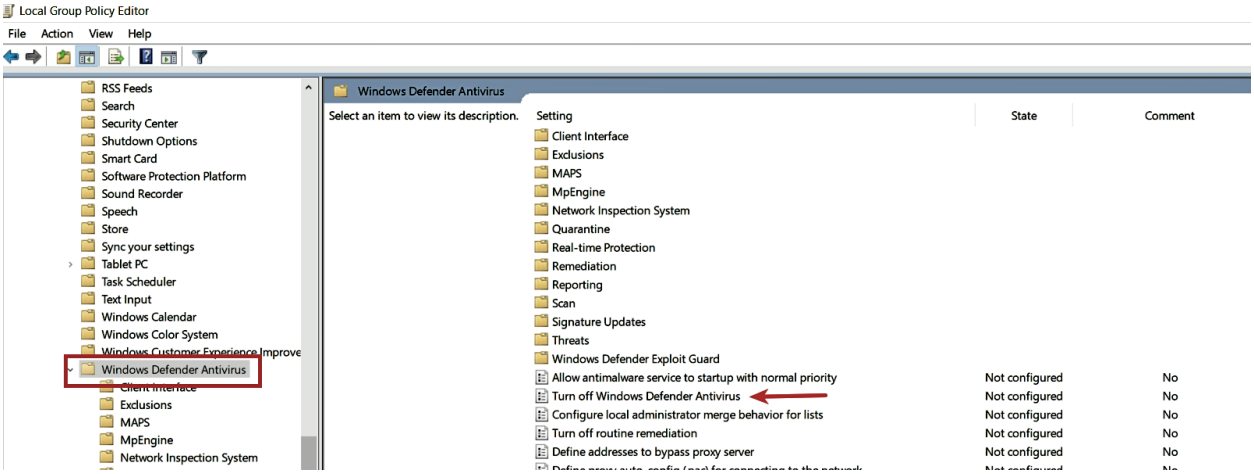
Launch the *Local Group Policy Editor* by Searching for *"edit group policy"* in the search box as shown in the following screenshot:



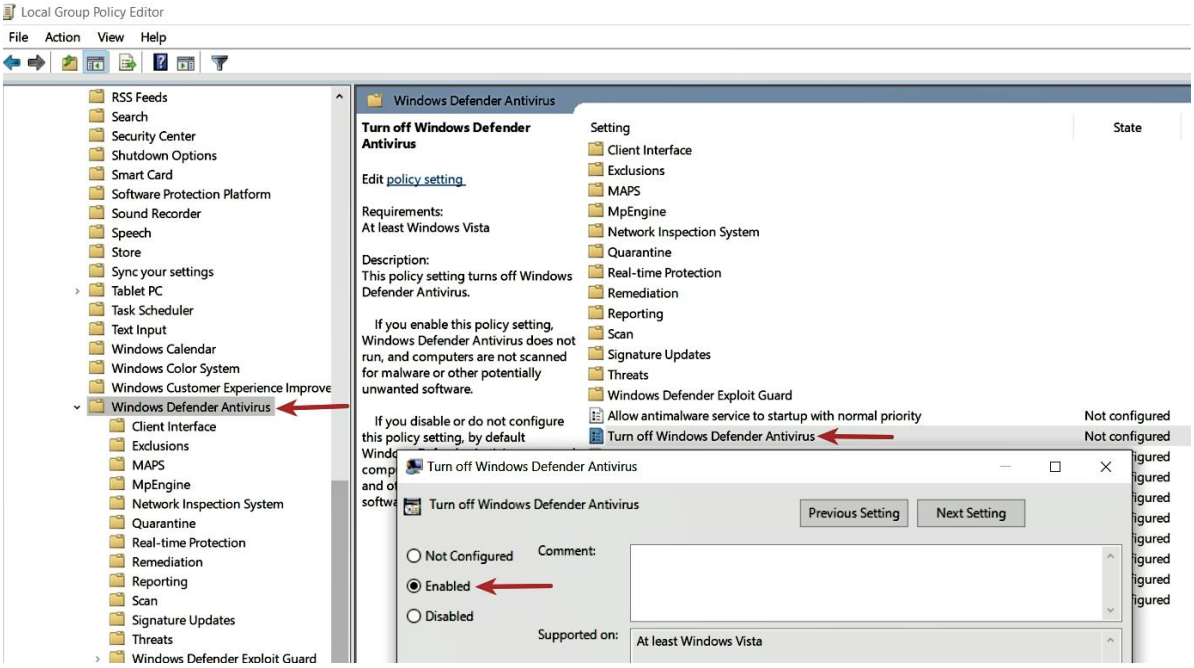
In the left pane of *Local Group Policy Editor*, navigate to the location mentioned below

Computer Configuration\Administrative Templates\Windows Components\Windows Defender Antivirus

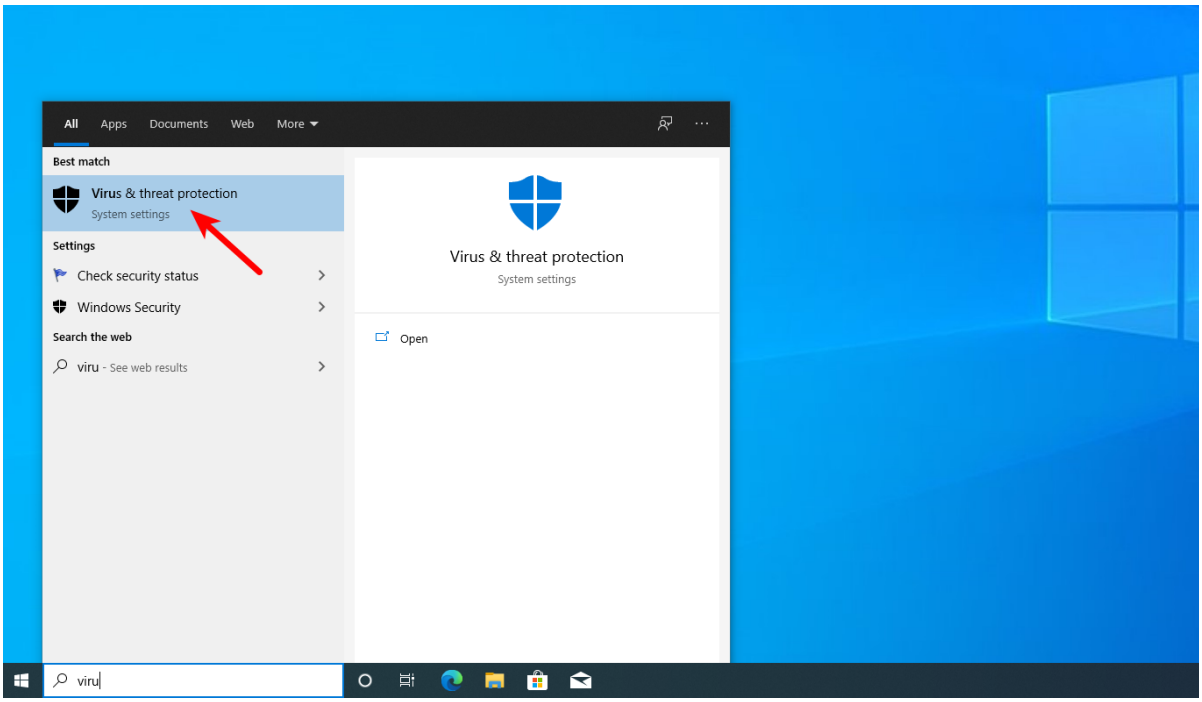
Note: On some older versions of Windows 10, "*Windows Defender Antivirus*" is just called "*Windows Defender*". In that case, navigate to ***Computer Configuration\Administrative Templates\Windows Components\Windows Defender*** and turn off "*Windows Defender*" using similar procedure.



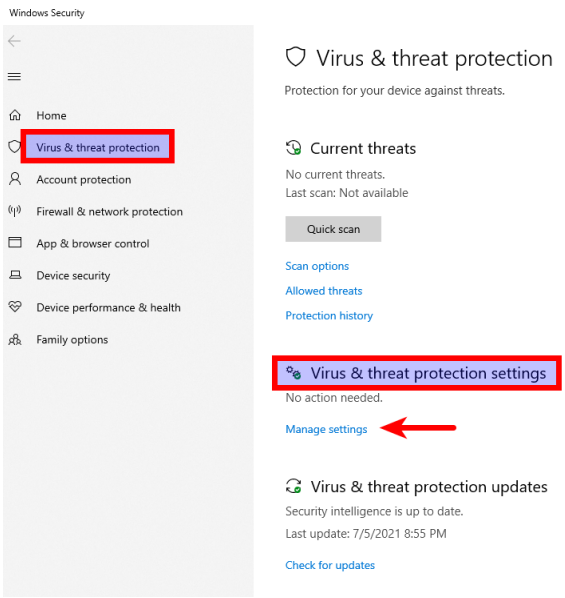
On the right pane of the "*Windows Defender Antivirus"*, double click on the "*Turn off Windows Defender Antivirus"* policy to edit it and then select *Enabled* and click on *OK* button. This setting will disable *Windows Defender Antivirus service*.

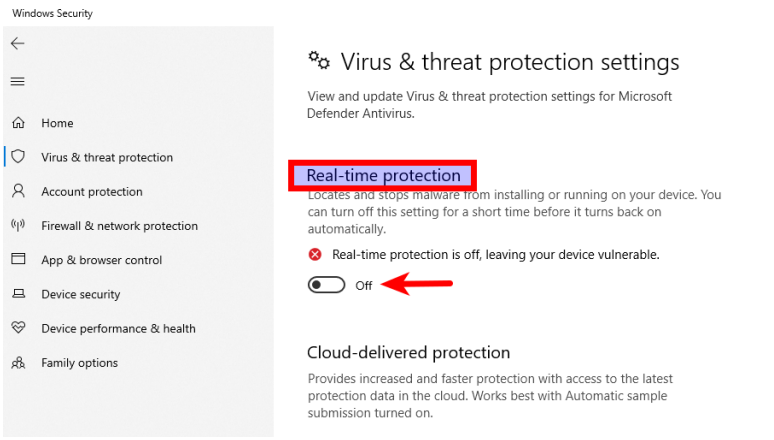


On some newer build versions of Windows, you are also required to disable *Real-time protection* (In addition to disabling *Windows Defender Antivirus*). To do that, bring up *"Virus & threat protection"* by searching for it in the search box.



Select *"Manage Settings"* located under *"Virus & threat protection settings"* and then turn off *"Real-time protection"* as shown in the following screenshots. (***Note:** On some older build versions of Windows you will not see these settings, in that case, skip this step and proceed with the next step*)





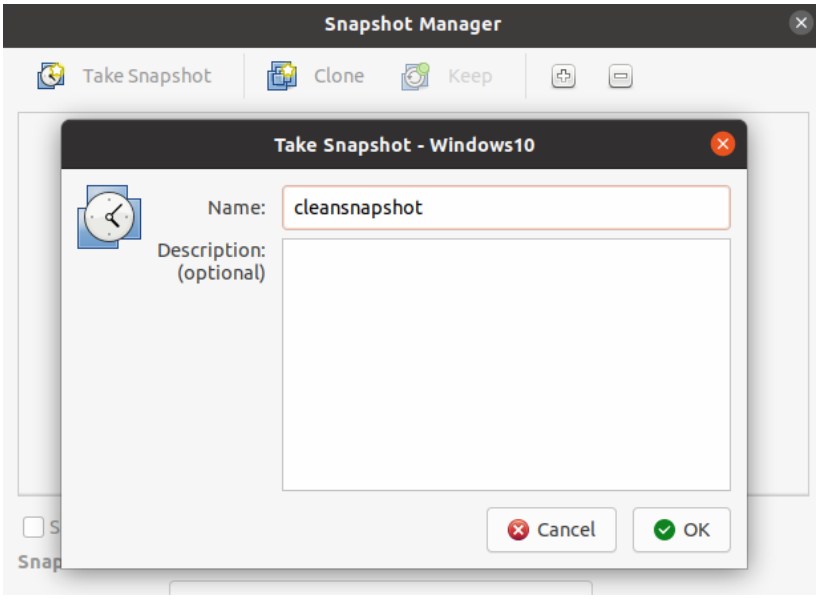
3) Download the Malware samples & Memory Images

During the training you will be analyzing various malware samples and investigating memory images. We recommend you download them in advance and keep them on your *host-machine* or copy it to your *VM instance of Windows*. The following are the download links to the malware samples and memory images

Malware Samples: *https://www.dropbox.com/s/u5vtjqveq847yun/malware_samples.zip?dl=0*

Memory Images: https://www.dropbox.com/s/ojaauwlpe4ppkyx/memory_images.zip?dl=0

At this point the lab environment is ready; please take a clean snapshot so that you can revert the VM back to the pristine/clean state after each analysis. Snapshot can be taken by clicking on ***VM -> Snapshot->Take Snapshot*** and give the snapshot a name of your choice (In the following screenshot we have chosen *"cleansnapshot"* as the snapshot name)



Now your lab setup is ready for the training. Thank you for taking time to setup the lab environment. We look forward to meeting you at the training.