Day 2- Setting Up the lab Environment

22 May 2022 20:33

Setting up an isolated lab environment is crucial before analysing malicious programs. While performing malware analysis, you will usually run the malicious code to observe its behaviour, so having an isolated lab environment will prevent the accidental spreading of malicious code to your system or production systems on your network.

Before Analysis of Malware we need to set-up the lab environment with the following tools:-

1- **Download Virtualization Software :-** (VMware / Virtual Box).

VMware:- https://www.vmware.com/go/getplayer-win

Virtual Box:- https://www.virtualbox.org/wiki/Downloads

2- **Windows ISO file :-** I choose windows platform because windows operating system are largely used and more targeted by attacker.

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

3- **FLARE VM :-** FLARE VM is free malware analysis VM with a ton of tools and features pre-installed by FireEye. It's a great addition to your malware analysis toolset.

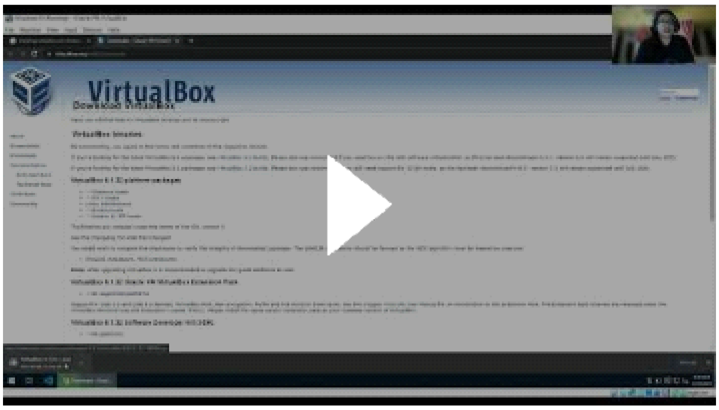
FLARE VM :- https://github.com/mandiant/flare-vm

4- **REMnux :-** REMnux is a powerful Linux VM that has a great collection of tools for Malware Analysis.

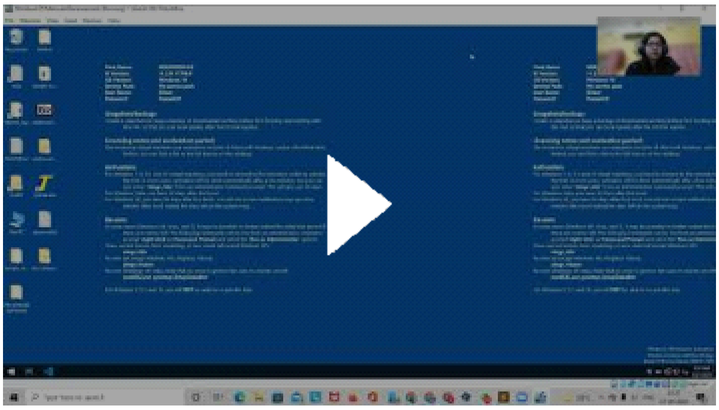
REMnux VM:- https://github.com/REMnux

following video link provide a step-by-step guide to set-up a lab environment.

1- Malware Analysis Basics - Lab SetUp & VM Installation



2- Malware Analysis Basics - Lab SetUp - FlareVm Installation



3- Malware Analysis Bootcamp - Setting Up Our Environment

4- How to setup FLARE VM on Windows 10