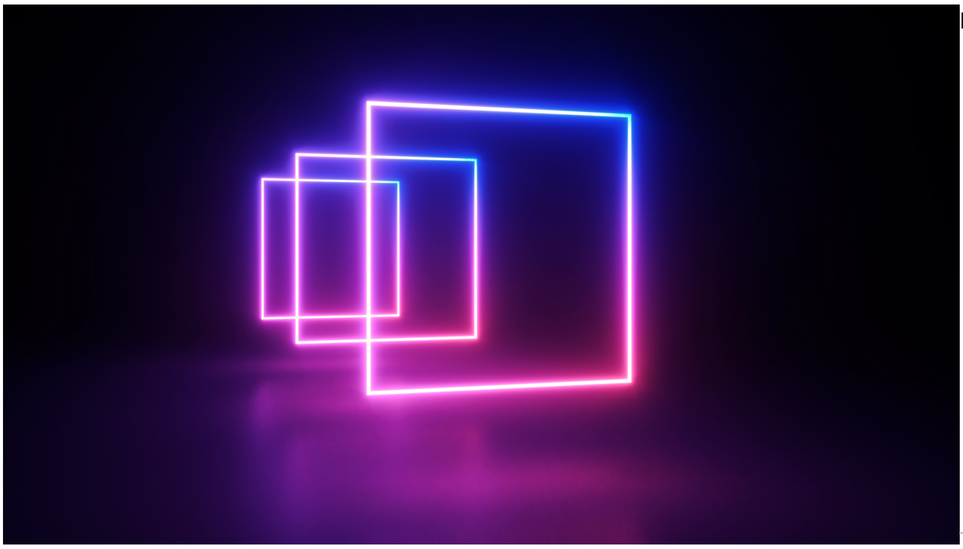
How to Get and Set Up a Free Windows VM for Malware Analysis



If you'd like to start experimenting with malware analysis in your own lab, here's how to download and set up a free Windows virtual machine:

- Step 1: Install Virtualization Software
- Step 2: Get a Windows Virtual Machine
- Step 3: Update the VM and Install Malware Analysis Tools
- Step 4: Isolate the Analysis VM and Disable Windows Defender AV
- Step 5: Analyze Some Malware

()

Step 1: Install Virtualization Software

Install virtualization software that you feel comfortable configuring and troubleshooting. VirtualBox (https://www.virtualbox.org/) and Hyper-V (https://docs.microsoft.com/en-us/virtualization/hyper-v-on-

MORE ON

Malicious Software (https://zeltser.com/malicious-software)

Technology (https://zeltser.com/technology)

Take a look at the malware analysis course (https://www.sans.org/course/reverse-engineering-malware-malware-analysis-tools-techniques) I teach at SANS Institute.

SHARE

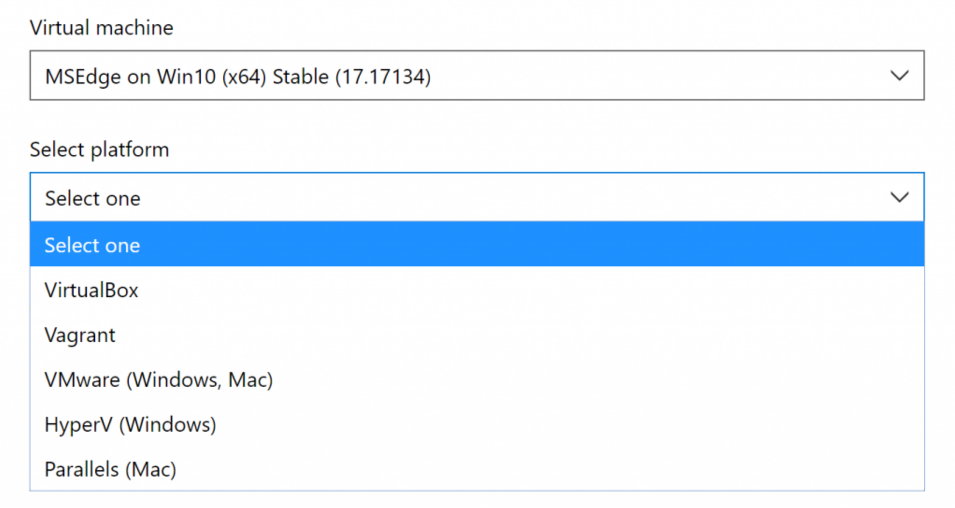
windows/quick-start/enable-hyper-v) are good free options. If you want to set up a headless server for your lab, you'll probably like VMware vSphere Hypervisor (https://www.vmware.com/products/vsphere-hypervisor.html) (formerly called ESXi), which is also free.

If using VMware Workstation, you'll need the commercial version: Workstation Pro (https://www.vmware.com/products/workstation-pro.html) for Windows and Linux or Fusion Pro (https://www.vmware.com/my/products/fusion-pro.html) for macOS. The free versions don't support snapshots. You'll want snapshots when examining malware, so you can revert the VM's state to start a new investigation or backtrack an analysis step. VMware provides a free 30-day trial.

()

Step 2: Get a Windows Virtual Machine

If you don't have a licensed version of Windows for your virtual machine, you can download a free Windows 10 VM from Microsoft. Go to the Microsoft Edge page for downloading virtual machines (https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/). Select "MSEdge on Win 10 (x64)" and pick the virtualization platform that matches the one you have:



Virtual machine

MSEdge on Win10 (x64) Stable (17.17134)

Select platform

Select one

If using macOS, you might be unable to extract the zip file's contents unless you download a file extractor such as The Unarchiver (https://theunarchiver.com/).

After downloading and extracting the archive, follow the steps appropriate for your virtualization software to start the VM. For example, for VMware you'd extract the files into a dedicated folder, then launch the file named "MSEdge – Win10.vmx".

The Windows OS in this VM expires after 90 days. Microsoft recommends "setting a snapshot when you first install the virtual machine which you can roll back to later."

The password Microsoft assigned to this virtual machine is "Passw0rd!" You won't need it for starting the VM, which will automatically log you in, but you might need to supply it when configuring the OS or installing software.

()

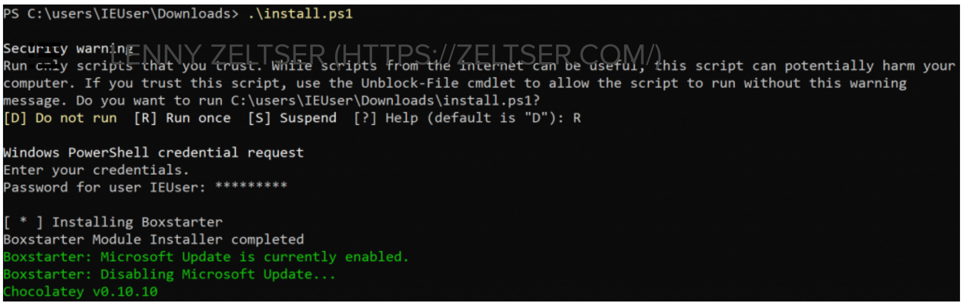
Step 3: Update the VM and Install Malware Analysis Tools

When you first boot the VM, it will be able to connect to the internet, assuming your physical host has internet access. You can use this connection to update the OS to the latest patch level and install malware analysis tools.

Next, install malware analysis tools. Here are some of my favorite free Windows tools for examining malicious software in a lab:

- Behavioral analysis: Process Monitor (https://docs.microsoft.com/en-us/sysinternals/downloads/procmon), ProcDOT (http://www.procdot.com/), Process Hacker (https://processhacker.sourceforge.io/), Wireshark (https://www.wireshark.org/)
- Code analysis: PeStudio (https://www.winitor.com/), IDA Freeware (https://www.hex-rays.com/products/ida/support/download_freeware.shtml), x64dbg (https://x64dbg.com/), Scylla (https://github.com/NtQuery/Scylla)

You can also automatically install lots of free malware analysis tools using the FLARE VM distribution (https://github.com/fireeye/flare-vm):



```
PS C:\users\IEUser\Downloads> .\install.ps1

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your
computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning
message. Do you want to run C:\users\IEUser\Downloads\install.ps1?
[D] Do not run  [R] Run once  [S] Suspend  [?] Help (default is "D"): R

Windows PowerShell credential request
Enter your credentials.
Password for user IEUser: *********

[ * ] Installing Boxstarter
Boxstarter Module Installer completed
Boxstarter: Microsoft Update is currently enabled.
Boxstarter: Disabling Microsoft Update...
Chocolatey v0.10.10
```

If you wish, install in the VM utilities such as VirtualBox Guest Additions and VMware Tools, which come with your virtualization software. They will make it convenient to share clipboard contents and files between your physical host and the VM. However, their presence slightly increases the chances that malware might detect the virtualized environment or manage to escape.

If you won't be using the file sharing methods supported by your virtualization software, decide how you'll transfer files in and out of the VM. Accessing a USB key from within the VM is a reasonable option. Another one is SFTP: You can enable the SSH server built into Windows (https://www.bleepingcomputer.com/news/microsoft/how-to-install-the-built-in-windows-10-openssh-server/), then access it from your physical host or from another VM using an SFTP client, such as WinSCP (https://winscp.net/).

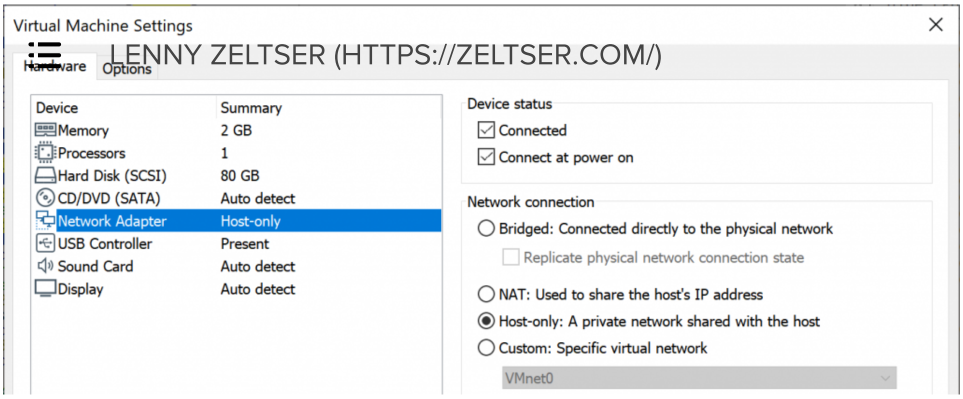
()

Step 4: Isolate the Analysis VM and Disable Windows Defender AV

Shut down your VM.

Consider disabling shared folders for the virtual machine, to make it harder for malware to escape. For example, to do that in VMware Workstation Pro, go to VM > Settings... > Options > Shared Folders and click Disabled.

Change the network settings for the VM so it doesn't have any network access. For instance, in VMware Workstation Pro you could put it into Host-Only mode by going to VM > Settings... > Hardware > Network Adapter and selecting Host-Only:



Virtual Machine Settings

Hardware Options

Device	Summary
Memory	2 GB
Processors	1
Hard Disk (SCSI)	80 GB
CD/DVD (SATA)	Auto detect
Network Adapter	Host-only
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Device status

☑ Connected

☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network

□ Replicate physical network connection state

○ NAT: Used to share the host's IP address

● Host-only: A private network shared with the host

○ Custom: Specific virtual network

VMnet0

A host-only network makes it possible for the VM to communicate with the virtual adapter of your physical host. For better isolation, consider defining a dedicated virtual network just for your virtual machine, then configure the VM to use that custom network. If you do this, then you won't be able to use SFTP to transfer files between the VM and your physical host.

Start your VM, now that it's no longer connected to the physical network.

Disable Windows Defender Antivirus inside the virtual machine, so the AV doesn't interfere with your malware analysis efforts. Use Group Policy to do this (https://www.windowscentral.com/how-permanently-disable-windows-defender-windows-10#disable_defender_gpedit) to avoid Windows periodically re-enabling AV. Optionally, use Group Policy to disable Windows Updates (https://www.howtogeek.com/224471/how-to-prevent-windows-10-from-automatically-downloading-updates/).

Once the VM is configured the way you like it, take a snapshot.

Be careful to avoid infecting the wrong system when analyzing malware and to minimize the chances that your specimen will escape. Strongly consider dedicating a physical host to such research; don't use this system for other tasks and don't connect it to a production network.

()

Step 5: Analyze Some Malware

You're ready to analyze some malware! I created lots of free resources for people looking to start learning malware analysis, in addition to the Reverse-Engineering Malware course (https://www.sans.org/course/reverse-engineering-malware-malware-analysis-tools-techniques) I teach at SANS Institute:

- Reverse-Engineering Malware Cheat Sheet (/malware-analysis-cheat-sheet/)
- Analyzing Malicious Documents Cheat Sheet (/analyzing-malicious-documents/)
- Tips for Reverse-Engineering Malicious Code (/reverse-engineering-malicious-code-tips/)
- Mastering 4 Stages of Malware Analysis (/mastering-4-stages-of-malware-analysis/)
- Introduction to Malware Analysis Webcast (/malware-analysis-webcast/)

Happy learning!

Updated March 4, 2019

DID YOU LIKE THIS?

Follow me for more of the good stuff.

About the Author

Lenny Zeltser develops teams, products, and programs that use information security to achieve business results. He is presently the CISO at Axonius and an author and instructor at SANS Institute. Over the past two decades, Lenny has been leading efforts to establish resilient security practices and solve hard security problems. As a respected author and speaker, he has been advancing cybersecurity tradecraft and contributing to the community. His insights build upon 20 years of real-world experiences, a Computer Science degree from the University of Pennsylvania, and an MBA degree from MIT Sloan.

Learn more (https://zeltser.com/about)