Malware Analysis Episode 1: Sharp Insights



**Reference:** [Malware Analysis In 5+ Hours - Full Course - Learn Practical Malware Analysis! - YouTube](https://www.youtube.com/watch?v=qA0YcYMRWyI) (by HusyHacks)

**TimeLine covered from the above video:** 38:40

**Caution:** Safe malware handling procedure is Critical. Safety is emphasized and must always be followed before analysing any malware sample.

**How to reach out to HuskyHacks:** DM on Twitter @HuskyHacksMK or email at [huskyhacks.mk@gmail.com](mailto:huskyhacks.mk@gmail.com)

**Key points:** on Setting up Lab for Malware Analysis (Safety)

1. Creating Virtual environment on your host machine for malware analysis. Good Virtualization applications are [VMware Workstation](https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html) or [Oracle VirtualBox](https://www.virtualbox.org/) which I prefer. Download them based on the Host OS + 32-bit/64-bit for system compatibility.
2. It is better if the guest OS installed in Virtual Machine is different from host OS to avoid any spread of infection. Example – Host OS is windows + Guest OS installed is Linux or Host OS is windows (Version A) + Guest OS installed is windows (Version B)
3. **Preference**: Guest OS installation should include Linux (Attacker- Remnux)+ [Windows 10](https://www.microsoft.com/ja-jp/software-download/windows10) (Victim + FlareVm) to conduct better analysis of the malware to stay updated with modern attacks techniques.
4. **Important:** Before starting any Malware Analysis activity, take Snapshot of your Guest OS in VM. Once you are done performing malware analysis these snapshots help you to revert to clean state of Guest OS that was taken before Malware testing was conducted. If anything goes wrong while performing malware analysis you can always revert to clean state of Guest OS.
5. Distributions useful to perform malware analysis – [Remnux](https://remnux.org/?ltclid=) (Linux Toolkit for malware analysis) or [FlareVm](https://www.mandiant.com/resources/blog/flare-vm-the-windows-malware) (windows malware analysis distribution) is installed on Windows
6. Network Adapter required for VM before starting Malware Analysis should be **Host-only Adapter (preferred).** (Network that is physically separated from our Host OS but logically connected for testing purpose, so that Guest OS cannot talk out of the VM to Host OS). Once the network settings are done, disconnect your device from the internet before detonating malware to avoid any unwanted communication with C2 panel/ External Websites.
7. **Crosscheck:** once you are done setting up the network in VM for testing**, try ping command** on Guest OS (Remnux & FlareVm on Windows) to check if Guest OS can reach out to Host OS/ External Website or IP. Ideally, Guest OS should not be able to reach out to your Host OS/ External Website or IP after setting up the Network Adapter to Host-Only. But The Guest OS systems (Remnux & FlareVm on Windows) should be able to ping each other for testing purposes. In short, Guest OS systems can talk to each other but not to the Internet.
8. If you are using Windows for malware analysis, make sure that your Guest Windows OS looks legit by installing common windows applications that you would use being a windows OS user. So that the malware is not able to detect the environment as Virtual Machine which will help us analyse the real behaviour/ Intentions of the malware.
9. In case of any Malware spread from Guest OS to Host OS, immediately disconnect your Host OS from Wi-fi connection/ Internet connection and enable **Airplane Mode** for device safety.
10. Some Malwares are designed in such a way to detect the environment it is trying to run on. Installation of **VMware Tools** is sometime detected by the malware confirming that the execution has taken place within a VM and not on Host OS. Avoid installing VMware Tools in your VM unless necessary and enabling direct Copy+ paste capability from Guest OS to Host OS. Also make sure to disable removal media insert in VM for safety reasons to prevent interaction with malware.

**Bonus Tip**: Keep your VM and Guest OS up to-date. If you are using Windows OS for malware analysis keep **Windows Update** and **Windows Defender** disabled while performing malware testing. If not done, windows will detect it as virus/malware and auto-remediation will take place here which will hinder your analysis.

Please let me know if this has helped you in any way. You can also add your views on lab safety through comments. I will be back next time with some more sharp insights on Malware Analysis Episodes.

-by Shefali Kumai

For more cyber security learning follow me here-

<https://www.youtube.com/channel/UCf-F-eATCUXYaUVk8Xl7OOQ>

<https://www.instagram.com/cybersecurity.cyber_seek/>

<https://twitter.com/Shefali37920461>