Risk	Mitigation
Malware reaches internet, and spreads into the wild	No direct internet access
Malware breaches hypervisor	Dedicated ESXI machine or live cd with disconnected drives (if at home). Modern and up to date hypervisor that is ring 3. Disabling of VMware tools. Defense in depth
Malware reaches local network	Use of virtualized custom network (no bridged!)
Malware persists on VM	Reverting to earlier snapshot / Scrubbing drive
Malware spreads in transit	Encrypted zips with password
Malware reaches router	No connected network cables or WIFI, static addressing
Malware spreads to shared folders	Avoid use of shared folders, have samples encrypted on snapshot, no downloads needed.
Malware detects VM, does not run	Install common apps, artificially use pc, increase RAM, remove additions/VMware tools, fake internet server (steps needed to bypass average VM checks)
Attacks act on the wrong target	All attacks will be done inside the virtualized network, that cannot reach the outside, this includes potential Kali/parrotOS. I will have a defined addressing scheme as part of the experiment