Build a Malware Lab

Local and Azure Cloud Security Considerations

Overview

Local Hypervisors

Local Hypervisors

VMWorkstation Pro

VMWare Workstation Player

KVM

ESXi

VirtualBox

Cloud Hypervisor

Azure Cloud

TBD

BUILDING THE MACHINE

BUILDING THE MACHINE - Local Hypervisor

RAM: Total RAM >= total VM RAM (Exception: KVM)

CPU: Total CPU > VM CPU use

NETWORK: (1) AVOID DISCLOSURE OF PERSONAL IP

(2) “NAT” to allow internet connection without seeing other devices on the network.

(3) “Host Only” .. [TBD]

BUILDING THE MACHINE - Azure Cloud

RAM: Cost oriented and/or enough RAM to mimic study environment

CPU: Cost oriented and/or enough to mimic authentic study environment

NETWORK: Do not allow traffic to public internet if malware behavior is unknown.

Ensure a DENY_ALL rule is placed for inbound/output bound connections in firewall

GUEST OPERATING SYSTEMS

GUEST OPERATING SYSTEMS

If running on old tech, be aware of the architectural relationship between the hypervisor machine and the VM OS. (I.E. x86 can only run 32-bit VMs)

Some labs are small and have only what is in-use.

Some labs have every OS under the sun. MalwareTech describes his lab as having every OS from Windows XP to 10 including 32-bit and 64-bit versions.

SNAPSHOT

Snapshot machine after first bootup.

Snapshot machine after installing software and any local configuration.

Snapshot machine after downloading malware.

Snapshot machine after executing malware.

ADVANCED

ADVANCED: Malware VM Detection

Harden VirtualBox to prevent malware from discovering it is operating in a virtual machine.

Hfiref0x - VBoxHardenedLoader