**Virtual Machine Weakness & Hardening**

**Remove all communication between host and guest**

* Bidirectional clipboard etc.
* These provide access to the host files and therefore provides an attack vector

VMs themselves can also have exploits of their own so they can’t be used without being configured/hardened or having other security controls in conjunction

Dedicated secure device for VMware in case of leak into host

Use a separate USB network dongle and place VM on separate network to host device

* Or physical network separation via VLAN

**Leak protect**

* HyperVisors can leave traces of their session use in log files etc.
* Its hard to know what files will be left by VMware so the mitigation is full Disk Encryption to make sure those files are unreadable
* Create a hidden (encrypted) OS where the hypervisor is installed and the guest VM is running
  + Plausible deniability
  + Although only provides security when machine is turned off as the encryption keys are stored in memory and therefore accessible when machine is off
* Disable audio and camera
* Disable shared folders, drag and drop, clipboard
* Disable video acceleration and 3d acceleration
* Disable serial ports
* Don’t install virtualbox guest addition or vmware tools
  + Gives the OS more access to hypervisor and vice versa – increases attack vector
* Remove flopper drives or cd/dvd drives
* Remove any viurtual disks
* Don’t attach any USB devices if possible
* Disable USB controller
  + Set pointing device to be PS/2 mouse
* Disable remote display server
* Disable I/O APIC
* Disable EFI
* Enable PAE/NX (security feature)
* Remove anything that’s not used

Use live OS (Convert Virtual disk image to ISO)

Use VM snapshots so you can return to snapshot state after doing any activities or contracting malware