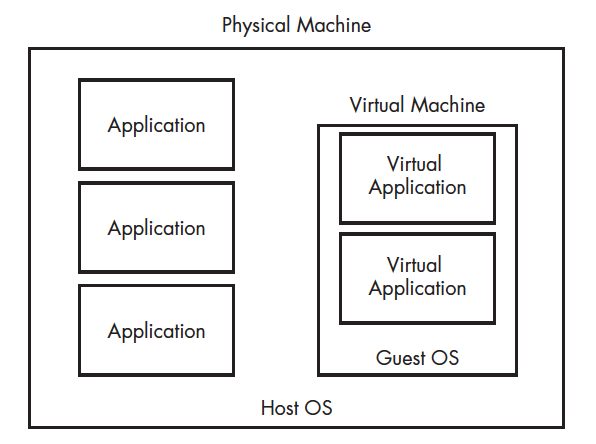
WEEK 2 – Chapter 2: ‘Malware Analysis in Virtual Machines’

Structure of a Virtual Machine

* A **computer** **within** a **computer**.
* Isolated from host OS, malware running on the virtual machine cannot harm the host OS.

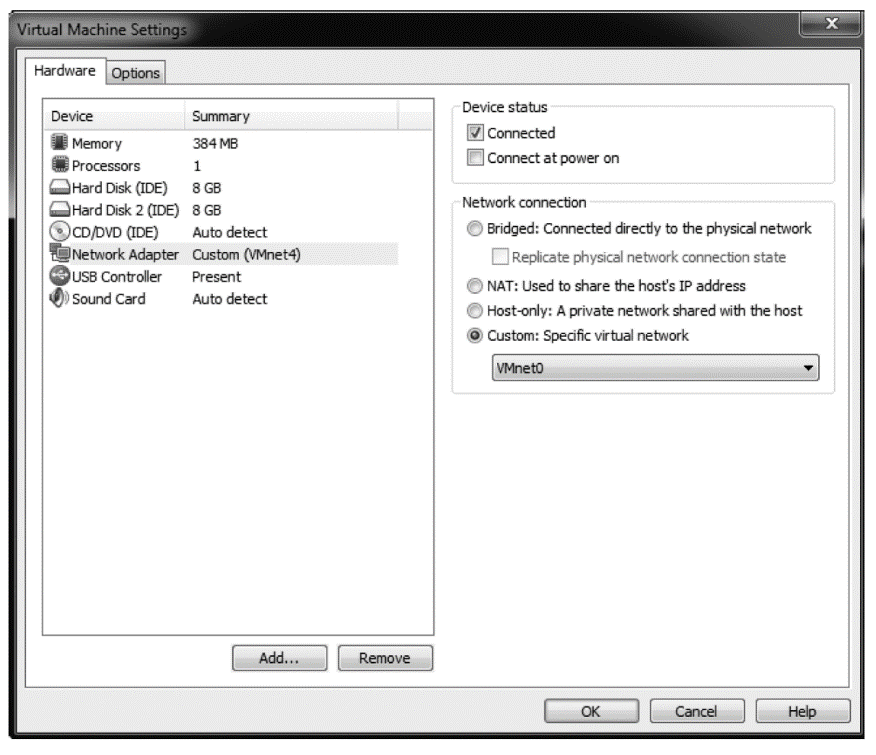


* **VMware Tools** offers a series of desktop virtualisation tools for analysing malware on virtual machines. Is also free.
* **VMware Workstation** is not free and is generally better for malware analysis.

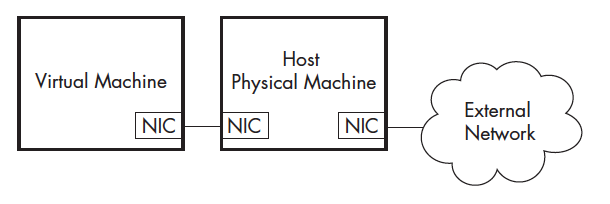
Creating a Malware Analysis Machine

**Configuring VMware**

* Most malware includes network functionality. A worm will perform network attacks against other machines in an effort to spread itself.
* When analysing malware, it is important to observe the malware’s network intentions, to create signatures or to exercise the program fully.
* VMware offers several networking options for virtual networking as shown beneath:



* You can disconnect the network by **VM > Removable Devices.**
* *Host-Only Networking:*
  + This creates a separate LAN between the host OS and the guest OS and is commonly used for malware analysis.
  + This LAN is not connected to the internet, which means it’s not connected to the internet but has some type of network connectivity as show beneath.



* *Multiple Virtual Machines:*
  + One last configuration combines the best of all options.
  + This makes use of multiple virtual machines linked by LAN but disconnected from the internet and host machine.
  + This ensures a network and the network is not connected to anything important.
  + When using more than one virtual machine for analysis, you’ll find it useful to combine the machines as a virtual machine team. When your machines are joined as part of a *virtual machine team*, you will be able to manage their power and network settings together.
  + You can create a virtual machine *‘team’* by selecting **File > New > Team**.
  + In this configuration, one virtual machine is set up to analyse malware, and the second machine provides services.

Using Your Malware Analysis Machine

* Sometimes you’ll want to connect your malware-running machine to the Internet to provide a more realistic analysis environment, despite the obvious risks.
* The biggest risk, of course, is that your computer will perform malicious activity, such as spreading malware to additional hosts, becoming a node in a distributed denial-of-service attack, or simply spamming.
* Another risk is that the malware writer could notice that you are connecting to the malware server and trying to analyse the malware.
* You should never connect malware to the Internet without first performing some analysis to determine what the malware might do when connected. Then connect only if you are comfortable with the risks.
* The most common way to connect a virtual machine to the Internet using VMware is with a **bridged network adapter**, which allows the virtual machine to be connected to the same network interface as the physical machine.
* Another way to connect malware running on a virtual machine to the Internet is to use VMware’s **Network Address Translation (NAT) mode**:
  + NAT mode shares the host’s IP connection to the Internet. The host acts like a router and translates all requests from the virtual machine so that they come from the host’s IP address. This mode is useful when the host is connected to the network, but the network configuration makes it difficult, if not impossible, to connect the

virtual machine’s adapter to the same network.

* + For example, if the host is using a wireless adapter, NAT mode can be easily used to connect the virtual machine to the network, even if the wireless network has Wi-Fi Protected Access (WPA) or Wired Equivalent Privacy (WEP) enabled.
  + Or, if the host adapter is connected to a network that allows only certain network adapters to connect, NAT mode allows the virtual machine to connect through the host, thereby avoiding the network’s access control settings.
* *Connecting / Disconnecting Peripheral Devices:*
  + To prevent worms from accessing devices such as USBs, VMware allows the option to disconnect devices. This can be done in the settings **VM > Settings > USB Controller** and unchecking the **Automatically connect new USB devices**.
  + This prevents USB devices from being connected to the VM.

Taking Snapshots

Taking snapshots is a concept **unique** to **virtual** **machines**. VMware’s virtual machine snapshots allow you **save a computer’s current state** and **return** to that point **later**, similar to a Windows restore point.

