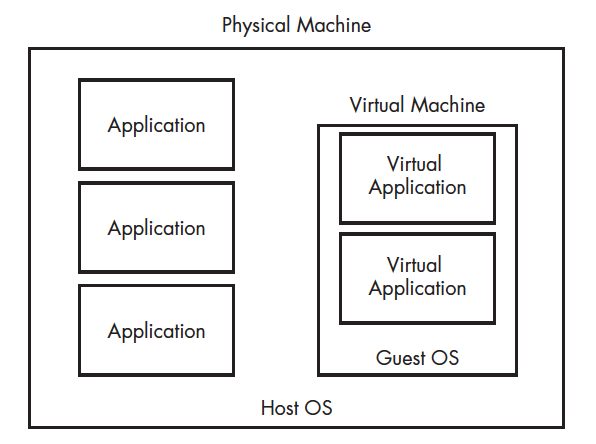
WEEK 2 – Chapter 2: ‘Malware Analysis in Virtual Machines’

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.

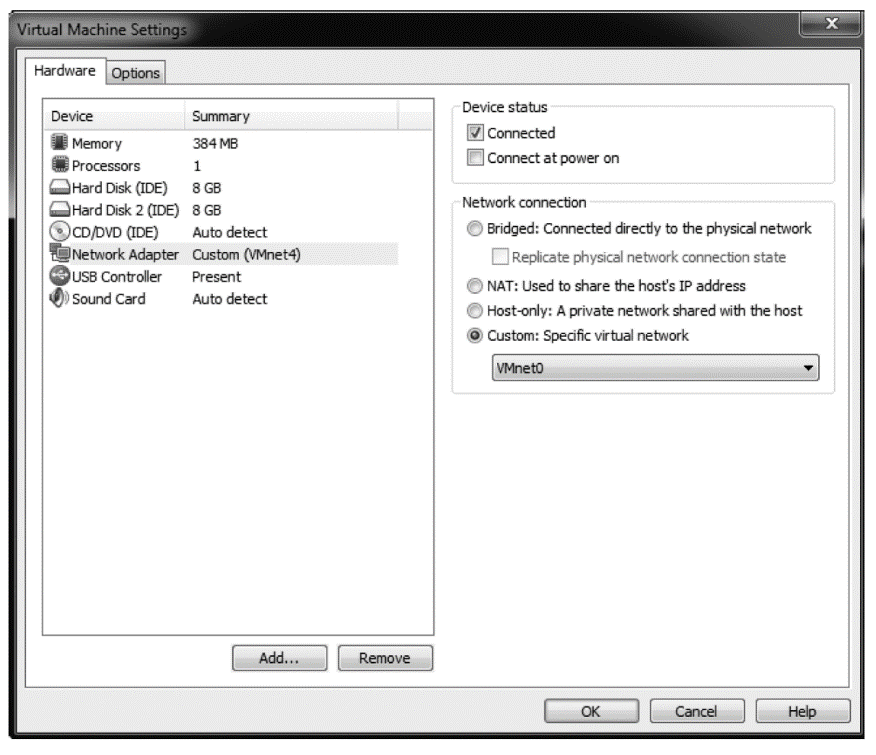


* **VMware Tools** offers a series of desktop virtualisation tools for analysing malware on virtual machines. Is also free.
* **VMware Workstation** is not free and is generally better for malware analysis.

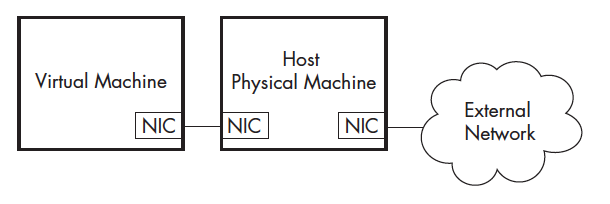
Creating a Malware Analysis Machine

**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

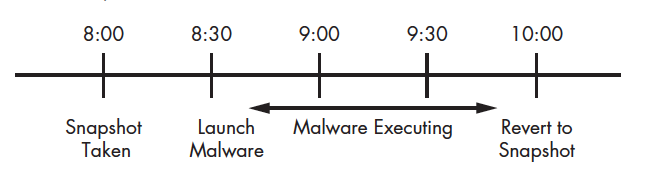
* Sometimes you’ll want to connect your malware-running machine to the Internet to provide a more realistic analysis environment, despite the obvious risks.
* The biggest risk, of course, is that your computer will perform malicious activity, such as spreading malware to additional hosts, becoming a 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.



After you’ve **installed** your **OS** and **malware** **analysis** **tools**, and you have **configured** the **network**, **take** **a** **snapshot**. Use that snapshot as your **base**, **clean-slate snapshot**.

Next, run your malware, complete your analysis, and then save your data and revert to the base snapshot, so that you can do it all over again.

VMware’s Snapshot Manager allows you to return to any snapshot at any time, no matter which additional snapshots have been taken since then or what has happened to the machine.

Transferring Files from a Virtual Machine

One drawback of using snapshots is that any work undertaken on the virtual machine is lost when you revert to an earlier snapshot. You can, however, save your work before loading the earlier snapshot by transferring any files that you want to keep to the host OS using VMware’s drag-and-drop feature. As long as VMware Tools is installed in the guest OS and both systems are running Windows, you should be able to drag and drop a file directly from the guest OS to the host OS.

The Risks of Using VMware for Malware Analysis

Some malware can **detect when it is running within a virtual machine**, and many techniques have been published to detect just such a situation. VMware does not consider this a vulnerability and does not take explicit steps to avoid detection, but some malware will execute differently when running on a virtual machine to make life difficult for malware analysts.

And, like all software, VMware occasionally has vulnerabilities. These can be exploited, causing the host OS to crash, or even used to run code on the host OS.

Although only few public tools or well-documented ways exist to exploit VMware, vulnerabilities have been found in the shared folders feature, and tools have been released to exploit the drag-and-drop functionality.

Record/Replay: Running Your Computer in Reverse

One of VMware’s more interesting features is **record/replay**. This feature in VMware Workstation **records everything** **that** **happens** so that you can **replay the recording at a later time**. The recording offers **100 percent fidelity**; **every** **instruction** that executed during the original recording **is** **executed** **during** a **replay**.

Even if the recording includes a **one-in-a-million race condition that you can’t replicate**, **it** **will be** **included in the replay**. VMware also has a **movie-capture feature** that **records** **only** the **video** **output**, but **record/replay** actually **executes** the **CPU** **instructions** of the **OS** and **programs**. And, unlike a movie, **you can interrupt the execution** **at any point** to **interact** with the **computer** and **make changes in** the **virtual machine**.

For example, if you make a mistake in a program that lacks an undo feature, you can restore your virtual machine to the point prior to that mistake to do something different.