Practical Malware Analysis

Chapter 2: M A L W A R E A N A L Y S I S I N V I R T U A L M A C H I N E S

Akbar Namin

Texas Tech University

Fall 2021

Reference:
Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software 1st Edition
by Michael Sikorski (Author), Andrew Honig (Author)

Run malware to perform dynamic analysis

- Running malware deliberately, while monitoring the results
- Requires a safe environment
  - machines on the network and be very difficult to remove

- Must prevent malware from spreading to production machines
- Real machines can be airgapped –no network connection to the Internet or to other machines
  - airgapped networks: isolated networks with machines that are disconnected from the Internet or any other networks to prevent the malware from spreading

Real Machines

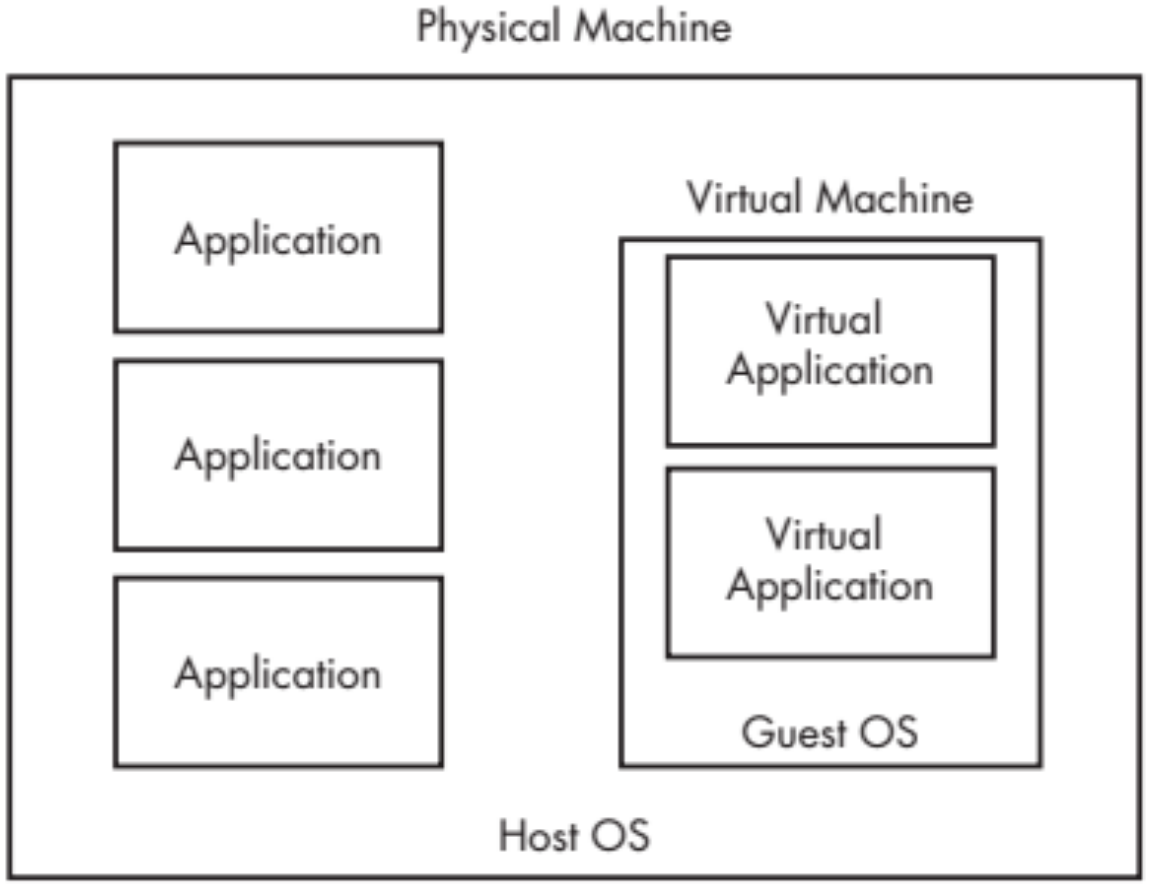
- Cons
  - No Internet connection, so parts of the malware may not work
  - Can be difficult to remove malware, so reimaging the machine will be necessary
- pros
  - Some malware detects virtual machines and won't run properly in one

Virtual Machines

- The most common method
- This protects the host machine from the malware
  - Except for a few very rare cases of malware that escape the virtual machine and infect the host

The Structure of a Virtual Machine

- Virtual machines are like a computer inside a computer
- OS running in the virtual machine is kept isolated from the host OS



Traditional applications run as shown in the left column. The guest OS is contained entirely within the virtual machine, and the virtual applications are contained within the guest OS.

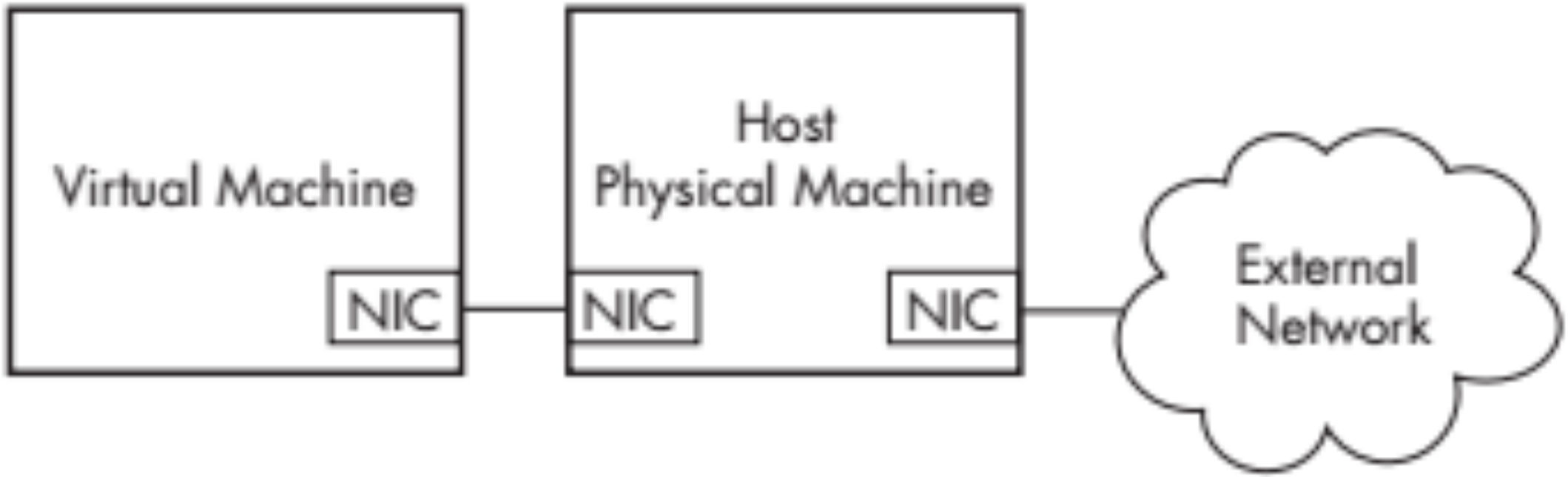
VMware Player

- Free but limited
- Cannot take snapshots
- VMware Workstation or Fusion is a better choice, but they cost money
- You could also use:
  - VirtualBox
  - Hyper-V
  - Parallels, or Xen

Creating Your Malware Analysis Machine

Configuring Vmware

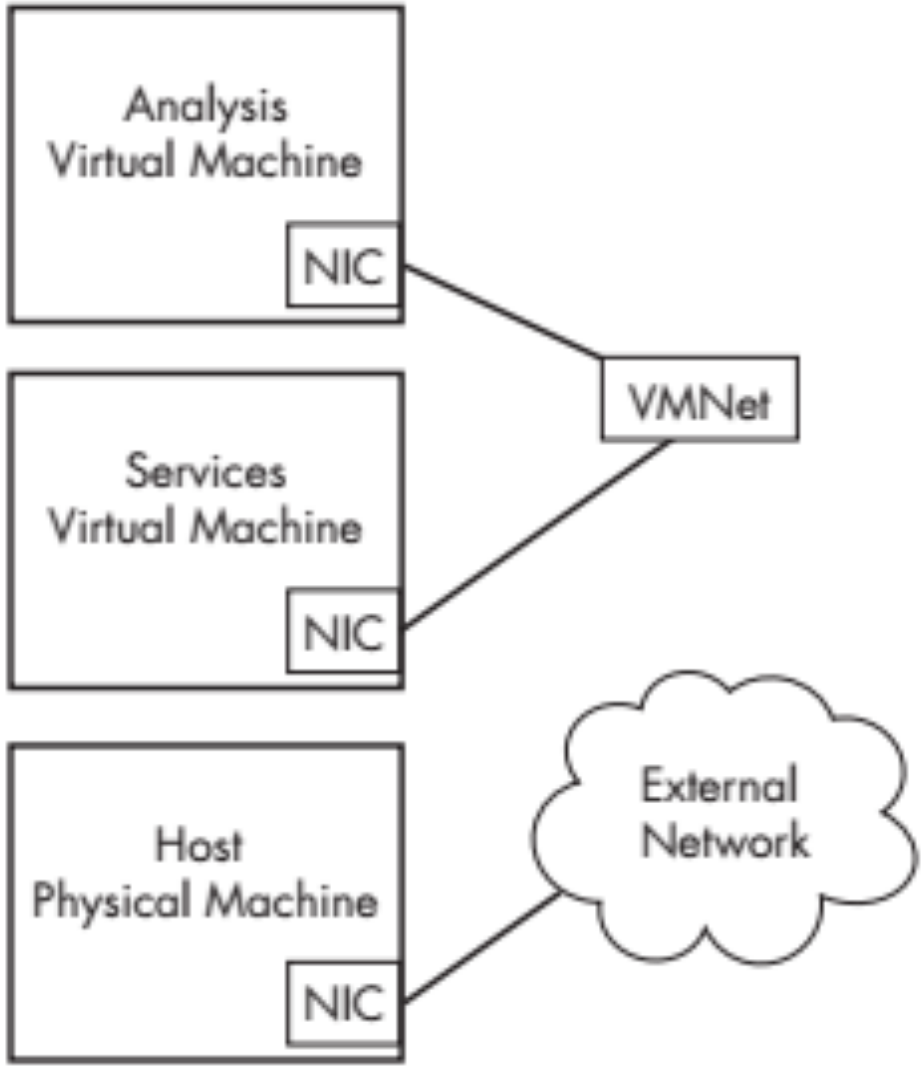
- You can disable networking by disconnecting the virtual network adapter
- Host-only networking allows network traffic to the host but not the Internet



Host-only networking in VMware

Using Multiple Virtual Machines

- This configuration combines the best of all options.
- It requires multiple virtual machines linked by a LAN but disconnected from the Internet and host machine
- malware is connected to a network, but the network isn't connected to anything important

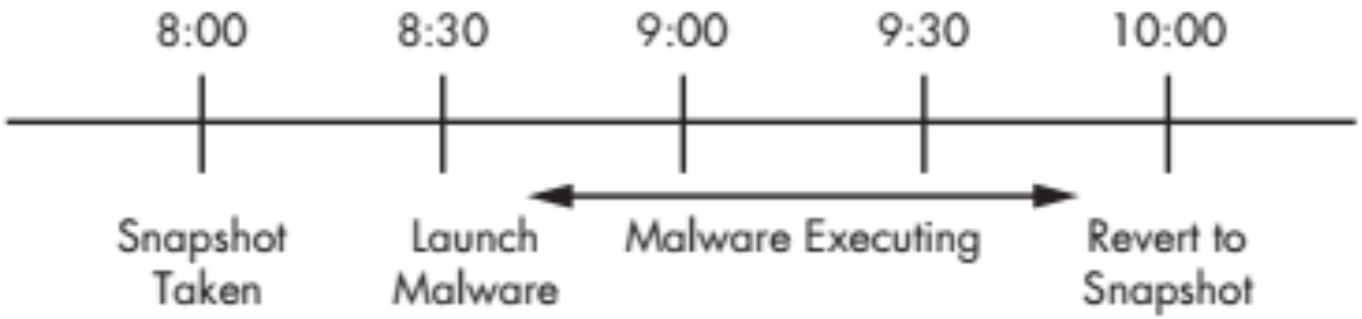


Connecting Malware to the Internet

- NAT mode lets VMs see each other and the Internet, but puts a virtual router between the VM and the LAN
- Bridged networking connects the VM directly to the LAN
- Can allow malware to do some harm or spread – controversial
- You could send spam or participate in a DDoS attack

Snapshots

- snapshots is a concept unique to virtual machines that allow you save a computer's current state and return to that point later, similar to Windows restore point



Snapshot timeline

Risks of Using VMware for Malware Analysis

- Malware may detect that it is in a VM and run differently
- VMware has bugs: malware may crash or exploit it
- Malware may spread or affect the host – don't use a sensitive host machine