School of

Engineering and Computer Science

Te Kura Mātai Pūkaha, Pūrorohiko

CYBR 473 T1 2022

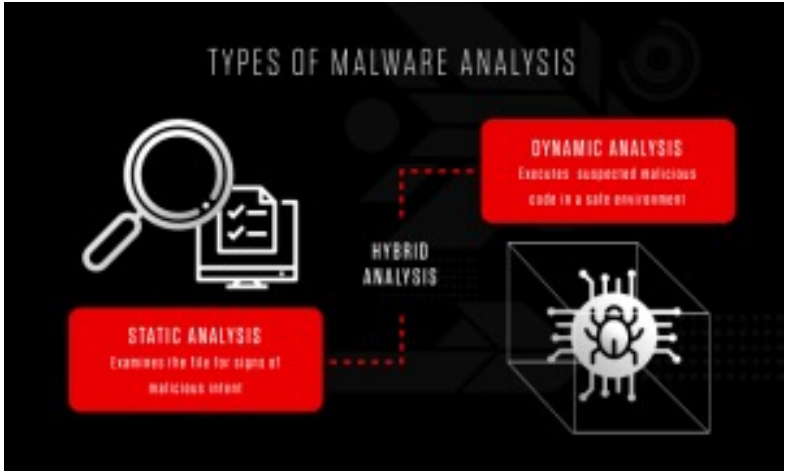
Malware and Reverse Engineering

Malware Analysis in Virtual Machines

Chapters 2&3: "*Practical Malware Analysis: The Hands-on Guide to Dissecting Malicious Software*", Michael Sikorski and Andrew Honig, 2012

Dynamic Analysis

- Running malware **deliberately**, while monitoring the results
- Requires a **safe environment**
- Must prevent malware from spreading to production machines
- Real machines can be **airgapped** –no network connection to the Internet or to other machines



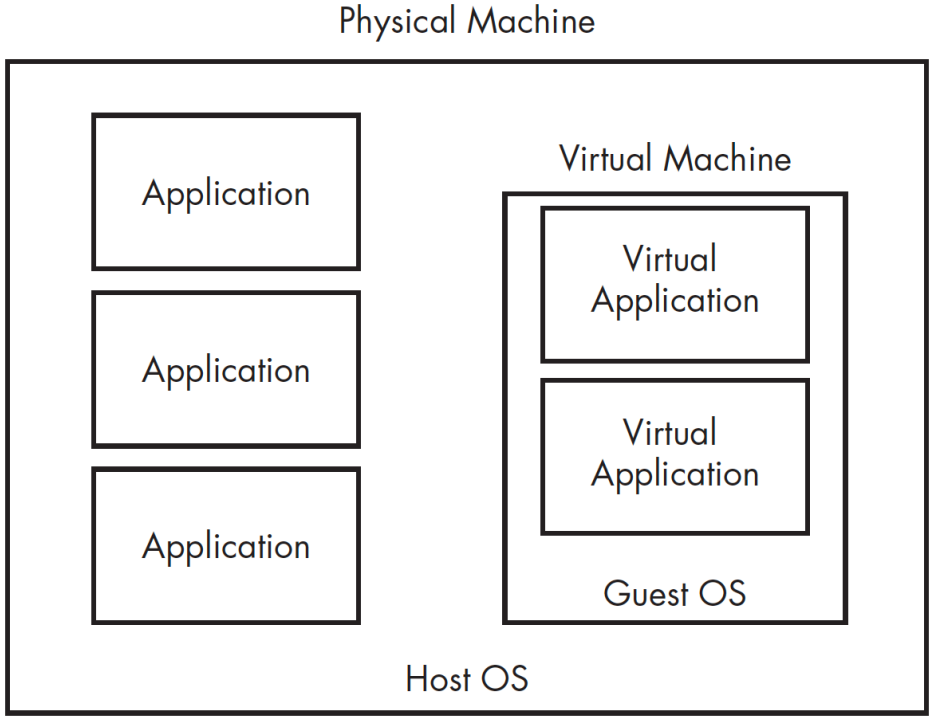
Real Machines

- **Disadvantages**
  - No Internet connection, so parts of the malware may not work
  - Can be difficult to remove malware, so re-imaging the machine will be necessary

- **Advantage**
  - Some malware detects virtual machines and won't run properly in one

Virtual Machines

- The most common method
- We'll do it that way
- 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



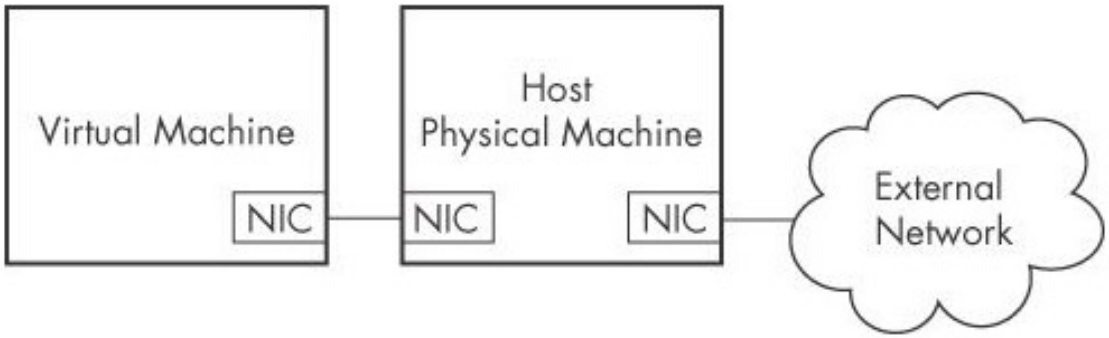
VMware Workstation Player/Fusion

- Free for education
- Cannot take snapshots

- You could also use VirtualBox, Hyper-V, Parallels, or Xen.

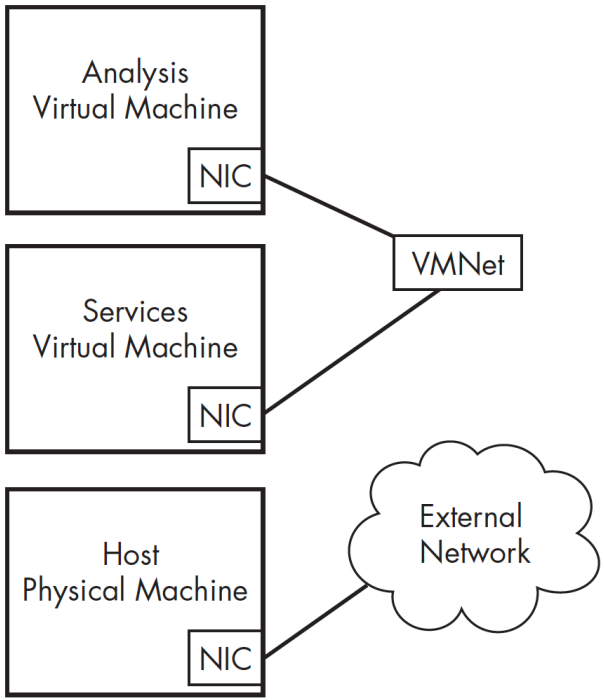
Configuring VMware

- You can disable networking by disconnecting the virtual network adapter
- You may want to enable the network connectivity when analysing malware (**why?**)
- **Host-only networking** allows network traffic to the host but not the Internet



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

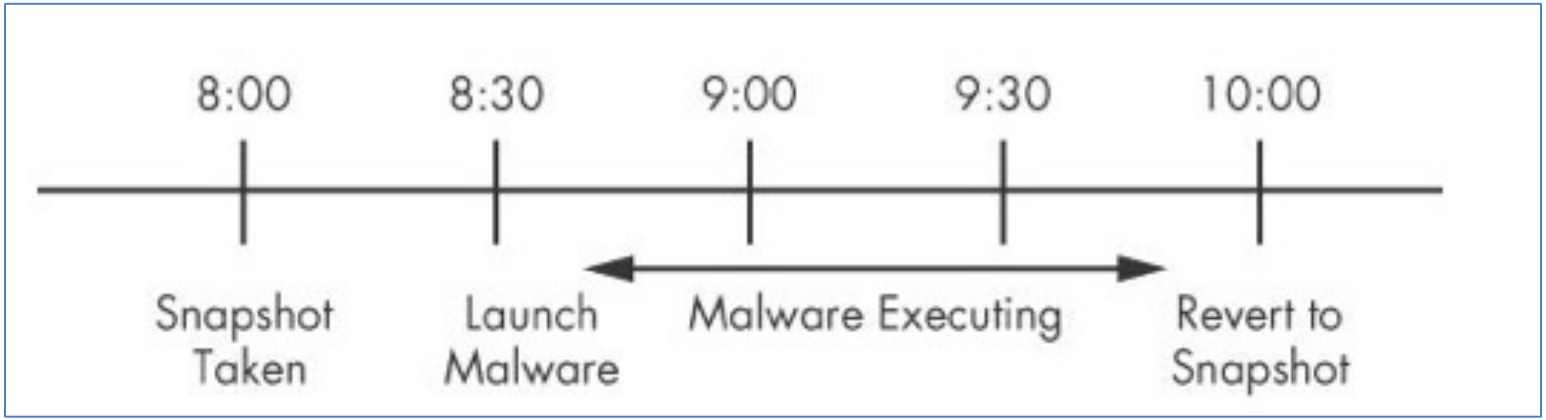


Peripheral Devices

- Can be connected to one but not both
- Issues with connecting peripheral devices, e.g., USB, automatically to the virtual machine

- Is there any potential issue if we do not connect **any** peripheral device to the virtual machine?

Snapshots



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
- **All the textbook samples are harmless**

BASIC DYNAMIC ANALYSIS

Why Perform Dynamic Analysis?

- Static analysis can reach a dead-end, due to
  - Obfuscation
  - Packing
  - Examiner has exhausted the available static analysis techniques

- Dynamic analysis is efficient and will show you exactly what the malware does
  - But there still some limitations with this approach!

SANDBOXES

Sandbox

- The quick-and-dirty approach
- All-in-one software for basic dynamic analysis
- Virtualized environment that simulates network services
- Examples: Norman Sandbox, GFI Sandbox, Anubis, Joe Sandbox, ThreatExpert, BitBlaze, Comodo Instant Malware Analysis
- They are expensive but easy to use
- They produce a nice PDF report of results

GFI Sandbox sample results for `win32XYZ.exe`

GFI SandBox™ Analysis # 2307
Sample: win32XYZ.exe (56476e02c29e5dbb9286b5f7b9e708f5)

Table of Contents

Sandbox Drawbacks

- No command-line options
- May not record all events (e.g. sleep)
- Other drawbacks
  - Malware often detects when it is running in a virtual machine
  - Some malware requires the presence of certain registry keys or files on the system that might not be found in the sandbox
  - If the malware is a DLL, certain exported functions will not be invoked properly
  - The sandbox environment OS may not be correct for the malware
  - A sandbox cannot tell you what the malware does

RUNNING
MALWARE

Launching DLLs

- EXE files can be run directly, but DLLs can't
- Use Rundll32.exe (included in Windows)

  `rundll32.exe` *`DLLname, Export arguments`*
- The *Export* value is one of the exported functions you found in Dependency Walker, PEview, or PE Explorer.

Launching DLLs (cont.)

- Example
  - rip.dll has these exports: **Install** and **Uninstall**
    rundll32.exe rip.dll, Install
- Some functions use **ordinal** values instead of names, like
  `rundll32.exe xyzzy.dll, #5`
- It's also possible to modify the PE header and convert a DLL into an EXE

END OF LECTURE. THANK YOU.