Practical Malware Analysis

Lecture 2 | Malware Analysis in Virtual Machines

Analysis Environment

Dedicated Hardware

- **Air-gapped** network
  - No Internet (or non-attributable connection)
- Difficult to revert

- Nullifies anti-vm techniques

Analyzing malware on dedicated hardware (bare metal) is somewhat uncommon

For a physical setup, you'd want to air gap the analysis machines from anything else, complete isolation from any other devices, including the internet

If you want to have internet connectivity, consider the risks involved (having an infected machine that may infect others, alerting a malware author to the fact you're analyzing the malware, etc) and consider a non-attributable network for the latter risk

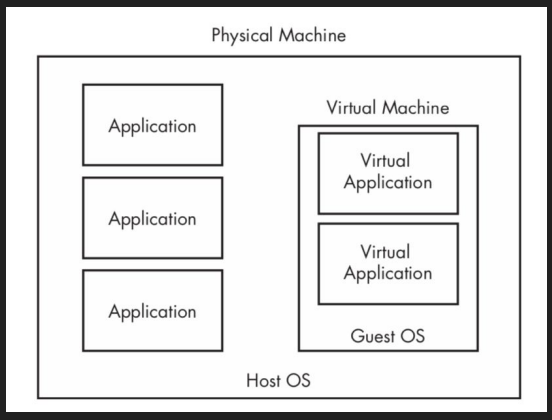
Physical machines are also difficult to restore to a clean state - malware may reach outside of the operating system for persistence and re-imaging a physical computer takes much longer than restoring a virtual machine

A pro to analyzing malware on a bare metal system is that it will most likely run normally, since any anti-vm techniques will not detect virtualization

Virtual Machines

A computer inside of a computer

- Uses the host's resources
- Able to be virtually isolated
- Easily revertable
- Shareable



- May trigger evasive behavior

Virtual machines are computers that are emulated inside of a host operating system

The virtual machines share the host's physical resources (RAM, hard drives, etc)

The virtual machine is able to be fully isolated from the host if desired (i.e not allowed to interact with files, applications, or devices accessible by the host)

Virtual machines are easily reverted via snapshots
Virtual machines are usually easier to share with other analysts than physical computers

Be aware that some samples may detect that they're being run in a virutal environment and change their behavior to avoid analysis

Virtual Machines

- VMware and VirtualBox most common
- VMware Workstation preferred for features
  - Install OS (Windows)
  - Default configs
  - Choose networking
  - Install analysis tools
  - Patch to desired level
  - Disable AV
  - Take snapshot

VMware and VirtualBox are some common virtualization tools - VirtualBox because it's free and VMware because it has a lot of handy features

Most analysts prefer VMware Workstation (or Fusion if your host is a Mac)

Windows is currently the most common target OS for malware, and therefore the most common analysis OS
Most default configuration options should work, adjust hardware allocations according to your host (VMware has dynamic options)
Choosing how to network your analysis VM can be difficult - covered on the next slide
Install your analysis tools, patch your VM to whatever level you need (if you're observing an old exploit it might be a good idea to use an analysis OS that is unprotected against that exploit)

Disable antivirus (like Windows Defender) so it doesn't eat your malware

Take a snapshot of your clean environment in order to revert to it between analyzing samples

Networking Options

- None
  - Secure
  - Miss vital network activity
- Host-only
  - No Internet but some network
  - Malware may spread to host

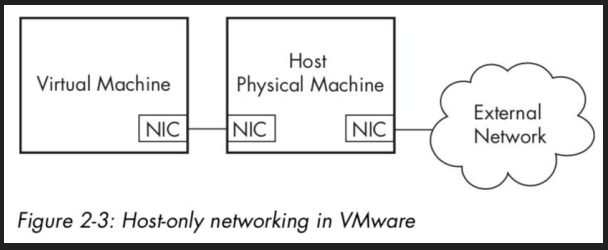


Figure 2-3: Host-only networking in VMware

While disconnecting your virtual machine from everything may seem like a smart move, it may also prevent you from observing important network activity during analysis

Host-only networking is a common option, as it disallows the VM any access to the internet, but does allow network access to the host for emulating services. VMware creates virtual network adapters for both the VM and the host to connect.

Host-only networking may pose a problem when running malware that attempts to spread across a network; it is a good idea to ensure your host is fully patched and implements restrictive firewall rules - but this may not protect against zero-day exploits

Networking Options

- Multiple VMs
  - Virtual adapters connected via a virtual switch
  - Isolated from host
  - One VM for service emulation
    - Simulate HTTP, DNS, etc
    - Set up as a VM team

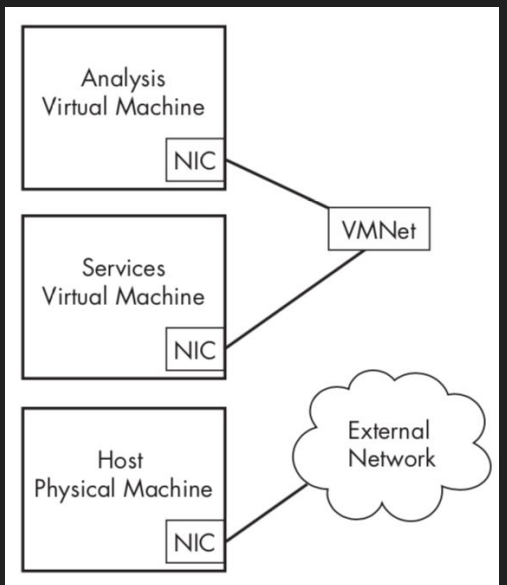


Figure 2-4: Custom networking in VMware

To get the best of both worlds (isolation and emulated network services) you can set up two VMs connected by a virtual switch
One VM may be used for malware analysis while the other provides network emulation to capture malware's network activity (HTTP, DNS requests, etc)

Setting up the VMs in a 'team' may be advantageous for keeping configurations identical between the two machines

Networking Options

Internet Connectivity

- Realistic
  - Good for analysis
  - Bad for other things on the Internet
  - Not stealthy
- Analyze first
- Bridged or NAT

Allowing an analysis VM to connect to the internet will provide the most realistic environment for network-enabled malware to operate in, however, this may include using your VM to perform malicious acts to other entities on the internet in order to spread or generate revenue for an author

Additionally, be aware that this malicious activity could be attributable to you (via your ISP or company) and may alert an attacker to the fact that someone has found and is analyzing their malware

Using a bridged network adapter will allow your VM to connect through the host's adapter using its own IP and MAC address
Using Network Address Translation will allow your VM to use the host machine as a router, sharing it's IP and MAC address (bypassing any extra authentication or access control issues)

Isolation

Be aware of connecting

- Peripheral devices
- Networks
- File systems
  - Shared folders
  - Drag and drop
  - Copy/paste

(Adjustable in your host’s settings)

Some malware may try to replicate or spread across connected networks, devices, and filesystems, nevermind VM escape exploits. It is important to know how your VM is allowed to interact with connected devices, the host filesystem, and any networked devices in order to prevent undesired contamination

Choose how your VM interacts with your host via its settings in VMware

Workflow

From a clean snapshot

- Load the malware onto the analysis VM
  - Re-adjust isolation settings if necessary
- Analyze the malware
  - Take snapshots along the way as desired
- Revert to clean

From a clean snapshot
Load the malware onto the analysis VM
Re-adjust isolation settings if necessary
Analyze the malware
Take snapshots along the way as desired
Remember to save any notes / work (I usually take them on the host OS if possible)
Revert to clean

Tips and Tricks

- VM escape exploits exist
  - Never analyze on an important system
- Record/replay
  - Removed in Workstation v8

VM escapes exist, it is important that your analysis VM exists on a machine that does not contain any sensitive personal/company information

VMware introduced a feature in VMware Workstation v6 that allowed a full capture and replay of every action performed during analysis, down the the processor instructions, which can be handy for analyzing self-modifying or destructive samples, though this feature was removed in version 8

Resources

Use VMware Workstation Player for a free tool to simply run VMs

Use VirtualBox as a free alternative to VMware (though lacking some features)

VMware Workstation and Fusion are not free but are recommended for serious analysis