Chapter 2. Malware Analysis in VMs
Virtual Machine (VM)

- VM – Software implementation of a machine that executes programs like a physical machine.
  - Abstraction layer – decouples the physical hardware from the operating system
  - Shares physical hardware resources with other users
  - Cloud Computing – share hardware resources (VM vs. Docker Container – all the dependencies for an application to run)
Sandbox

- A type of container: placed around an application.
- A virtual environment with restrictions.
VM – Cloud Computing

- Application
- Guest operating system (free BSD)
- Virtual CPU
- Virtual memory
- Virtual devices

- Application
- Guest operating system (Windows NT)
- Virtual CPU
- Virtual memory
- Virtual devices

- Application
- Guest operating system (Windows XP)
- Virtual CPU
- Virtual memory
- Virtual devices

Virtualization layer

Host operating system (Linux)

Hardware

CPU
Memory
I/O devices
VMs

- Most malware must be executed in order to analyze them
  - Running on production machine -> spread to others (worms)
    - Requires a safe environment with no risk

- **VirtualBox** and **Vmware**
  - Host-only networking to monitor network traffic
  - Snapshots and roll-back
  - Record and replay execution
VM Structure

Guest OS installed inside host OS as a VM
VM is isolated from the host OS
Host-only Networking

- Host-only networking: creates a separate private LAN between the host OS and the guest OS
- Malware is contained in VM, but not the Internet
Host-only Networking

There is no Internet connection

Your computer is offline.

DNS_PROBE_FINISHED_NO_INTERNET
Connecting VM to the Internet

- Default option in VirtualBox (NAT)
- NAT mode shares the host IP; host acts as a router and translates all the requests from VM
- In real malware analysis:
  - Cautious – spreading worm, becoming botnet for DDoS, spamming
  - Malware authors may notice you are connecting to the control server and trying to analyze
VM: Snapshot

- Snapshot is unique to VM
- Allows you to save the current state and possibly return to this state in future
- Extremely helpful in malware analysis
- Usually after you install all the tools, make a snapshot, or before you analyze some unknown program
Virtual Box Snapshot

- Under **Machine -> Snapshot**, view all the snapshots taken
Risks of using VM

- Malware can detect it is in VM and behave differently
- VM also have exploits, cause the host OS to crash or run the code on host OS (through the share folder possibly)
- Make sure the host OS is fully patched
- Avoid using a sensitive machine to perform malware analysis (save some of the non-personal files to the cloud like dropbox)
In-Class Homework

• Setup a Snapshot
• Run any program in the malware folder
• Rollback – restore to the previous snapshot when close the VM