CSCE 665: Lab Basics for VM

Guofei Gu

Virtual Machine

- Virtual Machine: a software implementation of a programmable machine(client), where the software implementation is constrained within another computer(host) at a higher or lower level of symbolic abstraction.[Wiki]

Virtual Machine in Security Research

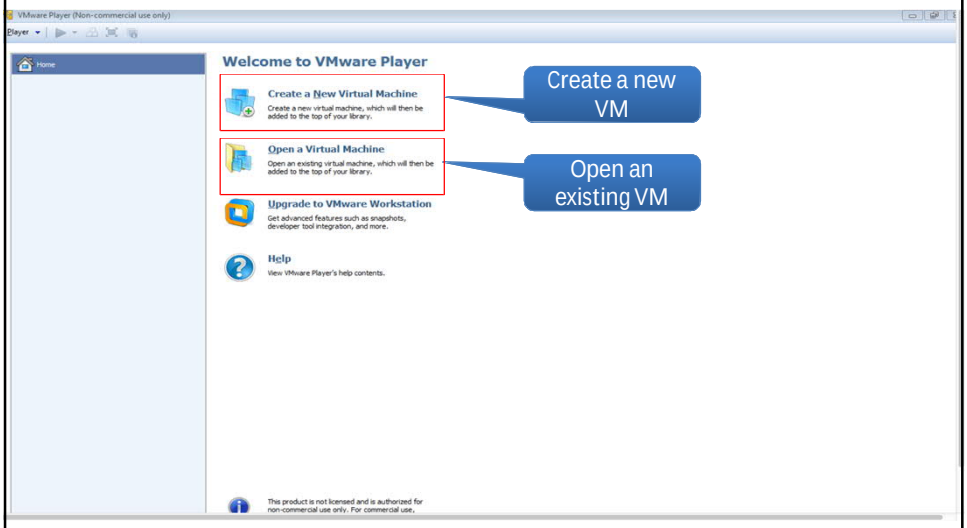
- You can run malware without damage!!
- No OS crash happened again!!!
- Honeynet and capture malware

- What you need to know:
  - How to create a virtual machine/virtual team
  - How to isolate your machine? And how to let them visit internet
  - How to create snapshot so you can recover from crash or malware infection.
- Software: Vmware Player/Virtual Box

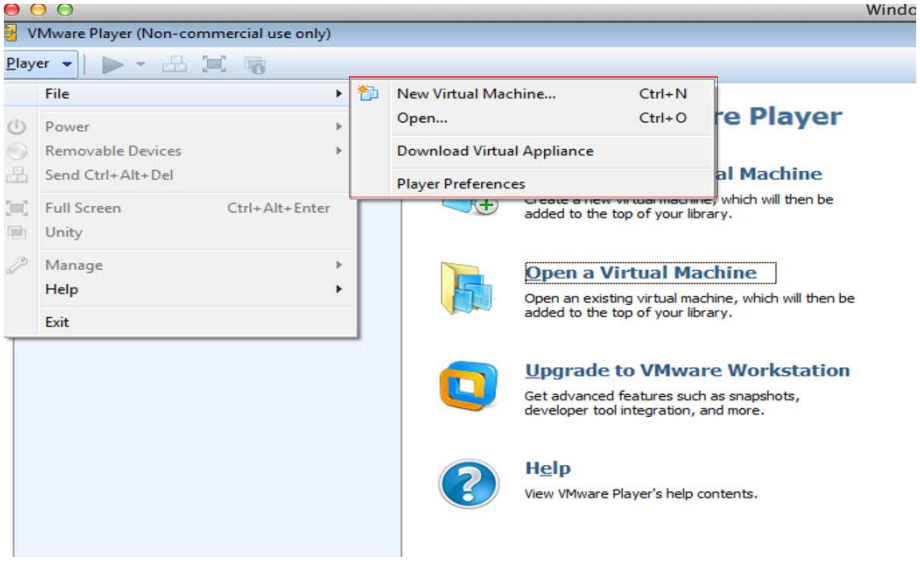
VMWare Player

- Free Software
- Run multiple OS at the same time on your PC
- Host OS: Windows 8, Windows 7, Chrome OS, Linux
- Download:
  - http://www.vmware.com/products/player/playerpro-evaluation.html

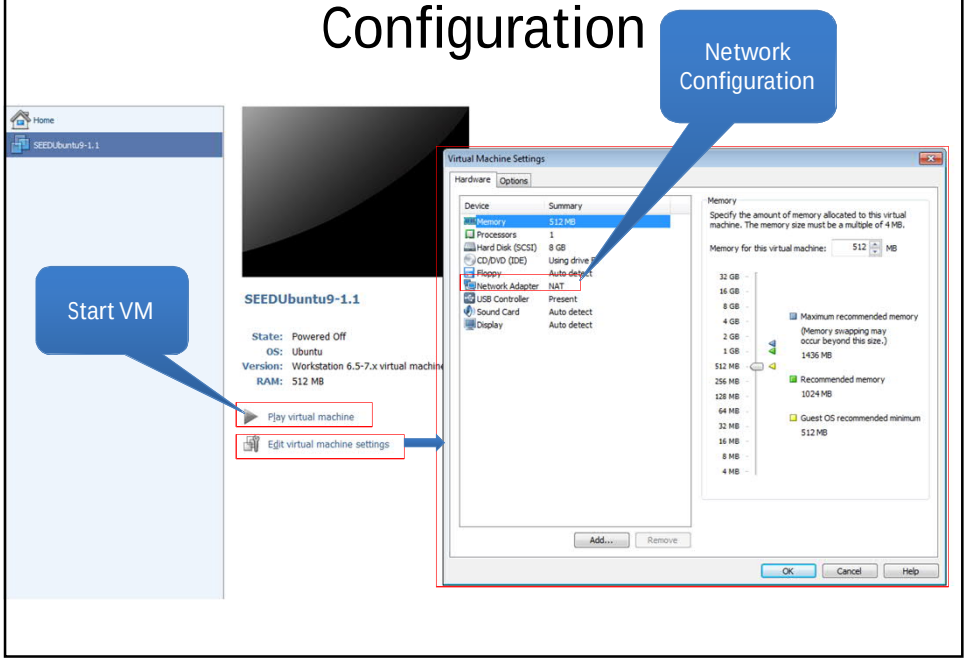
Cont.


Welcome to VMware Player
Create a New Virtual Machine
Open a Virtual Machine
Upgrade to VMware Workstation
Help
Create a new VM
Open an existing VM

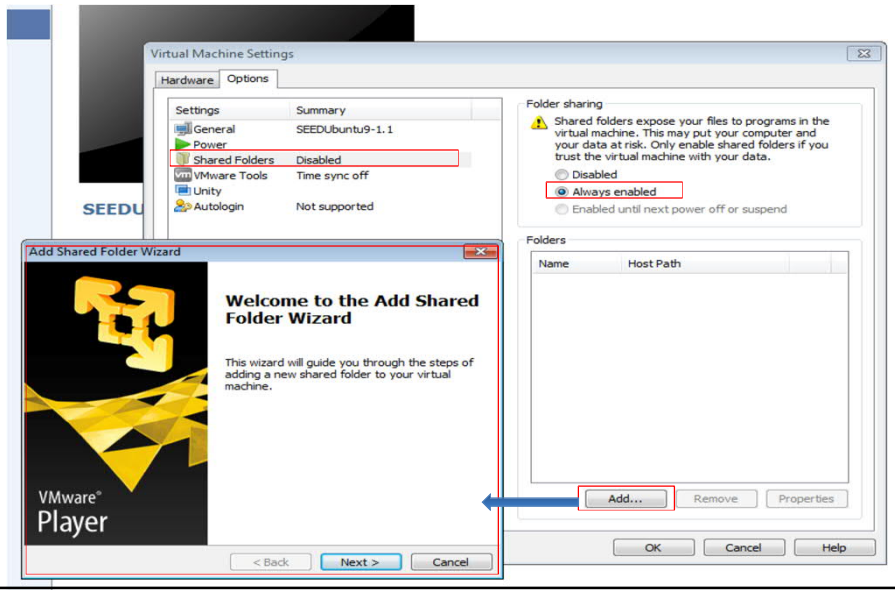
Cont.


VMware Player (Non-commercial use only)
Player
File
Power
Removable Devices
Send Ctrl+Alt+Del
Full Screen Ctrl+Alt+Enter
Unity
Manage
Help
Exit
New Virtual Machine... Ctrl+N
Open... Ctrl+O
Download Virtual Appliance
Player Preferences
Open a Virtual Machine
Open an existing virtual machine, which will then be added to the top of your library.
Upgrade to VMware Workstation
Get advanced features such as snapshots, developer tool integration, and more.
Help
View VMware Player's help contents.

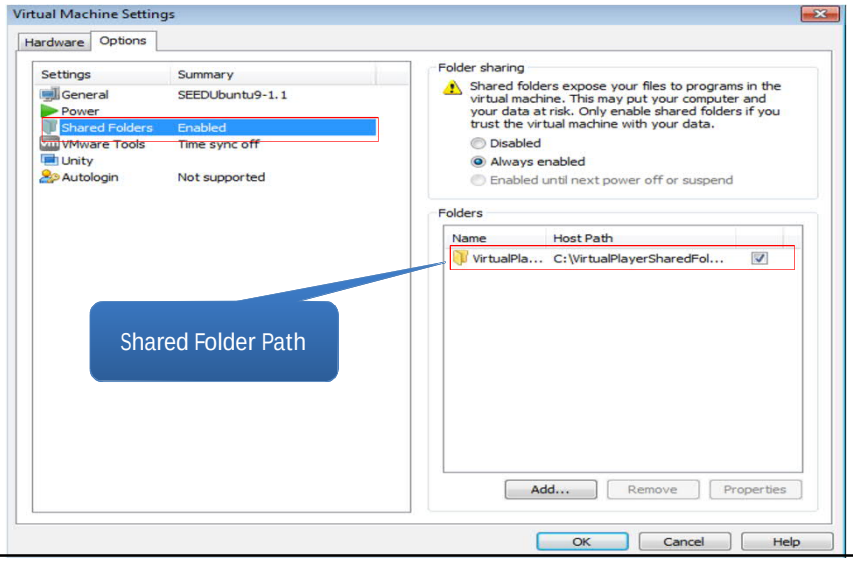
Configuration



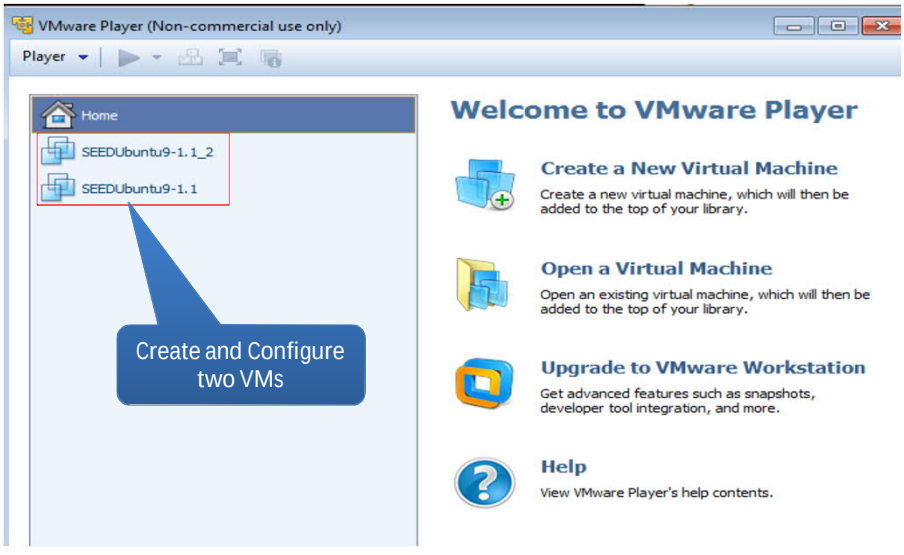
File Sharing with the host



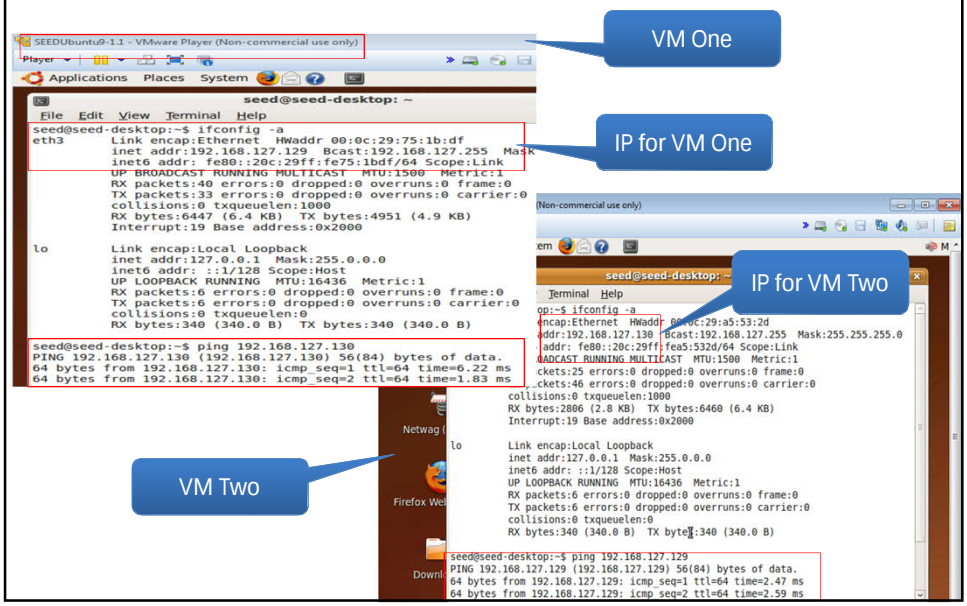
Contd.



Communication between two VMs

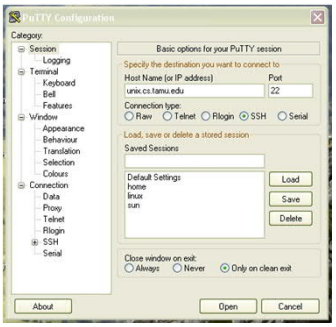


Communication between two VMs



Basic Unix/Linux programming

- Accessing CS systems
  - PuTTY (putty.exe) – a Telnet and SSH client
  - Common hosts:
    - unix.cs.tamu.edu
    - linux.cs.tamu.edu
  - Port 22 and SSH option
  - Accept key if prompted
  - Open and enter CS username and password



Common Commands

- ls – list current directory (ignores files that are 'invisible')
- cd *bob* – change directory to bob folder
  - cd .. (jumps one level up in directory)
- mkdir *filename* – makes a folder of given filename
- rm *blah* – removes file
  - rm **.ext* – removes everything in current directory of a given extension ext
- pwd – lists the path of the current directory
- other commands can be found at https://wiki.cse.tamu.edu/index.php/Basic_UNIX_Commands

File Editors

- As the directory you log into with unix and linux is the same as your H drive in most cases, you can modify files in a normal windows environment
  - Visual Studio, Notepad++, GVIM, etc.
- If you want to modify files in the putty system, common editors are pico (gives help at bottom) and vi (has more syntactical highlighting)
  - pico *filename*
  - vi *filename*

Compiling

- C programs
  - gcc *filename.c* - compiles and links c program, generating an executable file
- C++
  - g++ *filename.cpp* - compiles and links c++ program, generating an executable file
- Options for both
  - '-c' –compiles only, thus a main function is not needed
  - '-o' –renames the executable or compiled part in case of –c, thus your executable no longer must go under the a.out name

Debugging

- Unix/Linux debugger GDB
  - First compile and link your program (gcc or g++)
  - gdb *executable* – starts up gdb
  - run – executes the program and returns details about errors if any
  - For more info that concerns inserting breakpoints and stepping through your code look at http://www.unknownroad.com/rtfm/gdbtut/gdbtoc.html

Makefiles

- Makefiles are ways you can simplify compilation and linking on large projects by specifying once the order of linking/upkeep of the compilation process
- More info on creation and use of these files can be found at http://www.emba.uvm.edu/~snapp/maketutorial/make.html and http://frank.mtsu.edu/~csdept/FacilitiesAndResources/make.htm

Tools and Useful Reference

- C/C++ program IDE:
  - CodeBlock http://www.codeblocks.org/
  - Eclipse http://www.eclipse.org/
- Linux Programming References:
  - [Richard Stevens]UNIX Network Programming
  - [Neil Matthew] Beginning Linux Programming
- Vmware Network:
  - What is the differences among NAT, Host only and Bridge:
  - http://blog-rat.blogspot.com/2009/05/bridged-vs-host-only-vs-nat.html