FANSHAWE

INFO-6003

O/S & Application Security

Week 01

FANSHAWE

Agenda

- Contact Information
  - Professor S.J. Freymond
- Basic Concepts of Virtualization
  - Bare-Metal Hypervisor
  - Host-Based Virtualization
  - VMWare Workstation
- Setting up a folder structure that works well with virtual machines in a multi-class environment

Contact Information

- Email
  - Use my FOL email address
    - sfreymond@fanshaweonline.ca
  - Email sent Monday to Friday
    - You can expect a turnaround of 48 hours or less
  - Email sent on the Weekend
    - I usually check my email Sunday evening or first thing Monday morning

Contact Information

- Email Tips
  - Use a relevant Subject
  - Keep it brief and to the point
  - Don’t be afraid to use point form
  - Try not to wait until the last minute to send your email

FANSHAWE

Course Information

- This course will provide an overview of, and concentrate on, the essential concepts of information security, specifically:
  - Vulnerabilities of Windows and Linux Operating Systems
  - Upgrading and Patching
- This course is a prerequisite for:
  - INFO6009 – Network Monitoring & Penetration Testing
  - INFO6065 – Ethical Hacking & Exploits

Course Information Sheet

- Learning Outcomes
  - What you are expected to be able to demonstrate that you have learned
  - Questions on tests will reflect these items
    - Lecture and Lab Content
- Detailed Content
  - What you should expect to be taught each week
  - Content, tests, labs
- Course Textbook
  - Suggested and Required textbook
- Methods of Evaluation

FANSHAWE

How to Succeed in This Course

- Reading the Slides and listening to lectures will most likely get you a F in this course.
- Additionally, doing the labs in class every week may get you to a D - 50%
- Additionally, taking Notes in the lectures may boost you to a C - 60%

How to Succeed in This Course

- Additionally, spending at least 4 hours every week studying the above material and doing the assigned readings may earn you a B - 70%
- If you want to get an A or higher:
  - Doing all of the previous, then going above and beyond:
    - Research
    - Study groups and quiz groups
    - Making your own questions to study from
    - Redoing labs
    - Flash cards
    - Listening to MP3 versions of your notes/course lectures

FANSHAWE

Course Information

- This course is delivered to both students in class and online: through interactive web sessions
- Online students will be able to ask questions via interactive text chat
  - I will check the chat periodically throughout the lecture/lab
- Each lesson will be recorded and available through the Virtual Classroom link in FOL

FANSHAWE

Course Information

- The course is assigned 4 hours per week
- 2 hour lecture followed by a 2 hour lab
- The labs will develop essential skills and reinforce the lecture content

Method of Evaluation

- Tests and Exams: (65%)
  - Details can be found on the Course Information Sheet
- Labs (35%)
  - Labs are delivered weekly and need to be completed during the lab period for in class students
    - Online students have until the night before the next lab to complete the lab
  - Lab Marking Details can be found in the Additional Course Information Section

Lab Expectations

- Deduction for late arrival
  - I put a sign in sheet out when I arrive in the classroom
  - You have the opportunity to sign in while I am setting up
  - Once I start the lab I remove the sign in sheet and you are considered late
    - 25% deduction for late arrival

Lab Expectations

- Submission Times
  - To be eligible for full marks you need to submit your lab during the lab period (in class students)
  - Marks will be deducted for mistakes
  - The lab period ends ten minutes before the hour
    - 1 minute late, is late
  - If you submit the lab late it will be marked out of 50%
  - You have until midnight, on the day of the lab to submit it late
- The official rules can be found in the Additional Course Information section on FOL.

FANSHAWE

What is Virtualization?

- A technology that provides an abstraction of the resources used by some software which runs in a simulated environment called a virtual machine (VM)
- Benefits include better efficiency in the use of the physical system resources
- Provides support for multiple distinct operating systems and associated applications on one physical system
- Raises additional security concerns

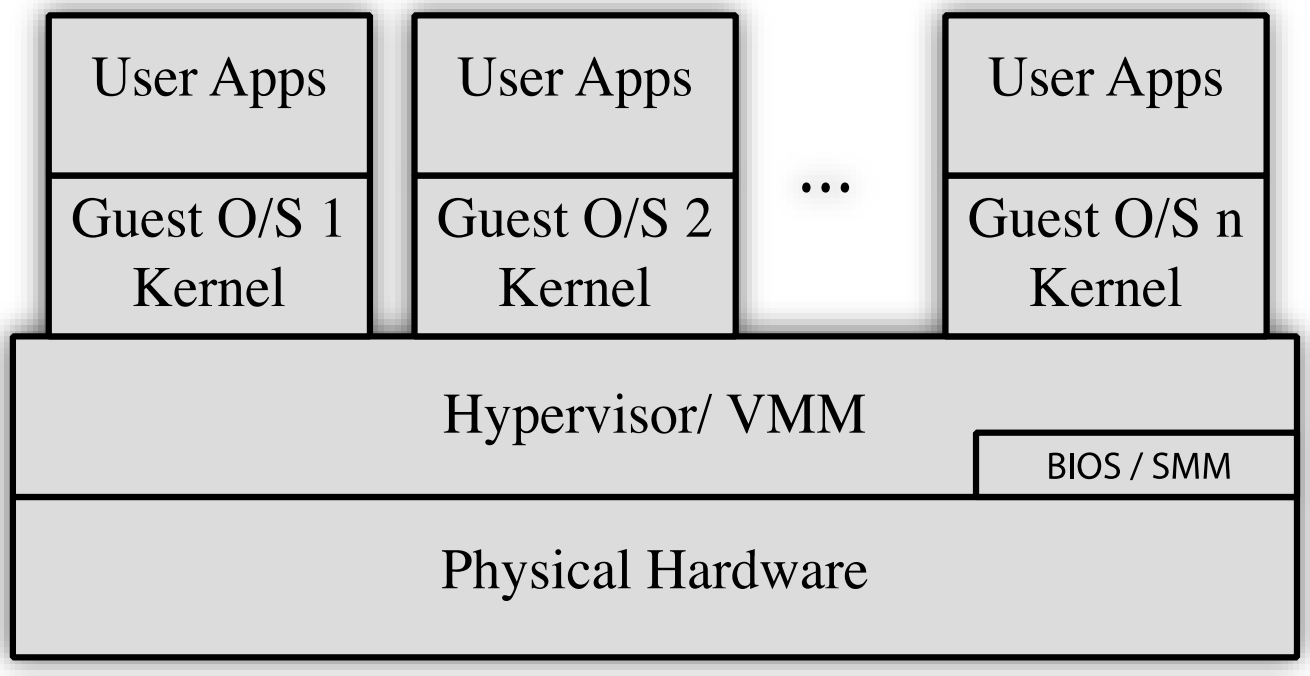
FANSHAWE

Types of Virtualization

- Type1
  - Also known as a Bare Metal Hypervisor
  - The hypervisor is installed directly onto the hardware
  - The hypervisor has more direct access to the hardware
    - More Efficient, but More Expensive
- Type 2
  - Referred to as Hosted, Host based, or OS based
  - The hypervisor is running on top of another operating system: Windows, Linux, OSX
  - The OS is sitting between the hypervisor and the hardware
    - Less Efficient, but Less Expensive

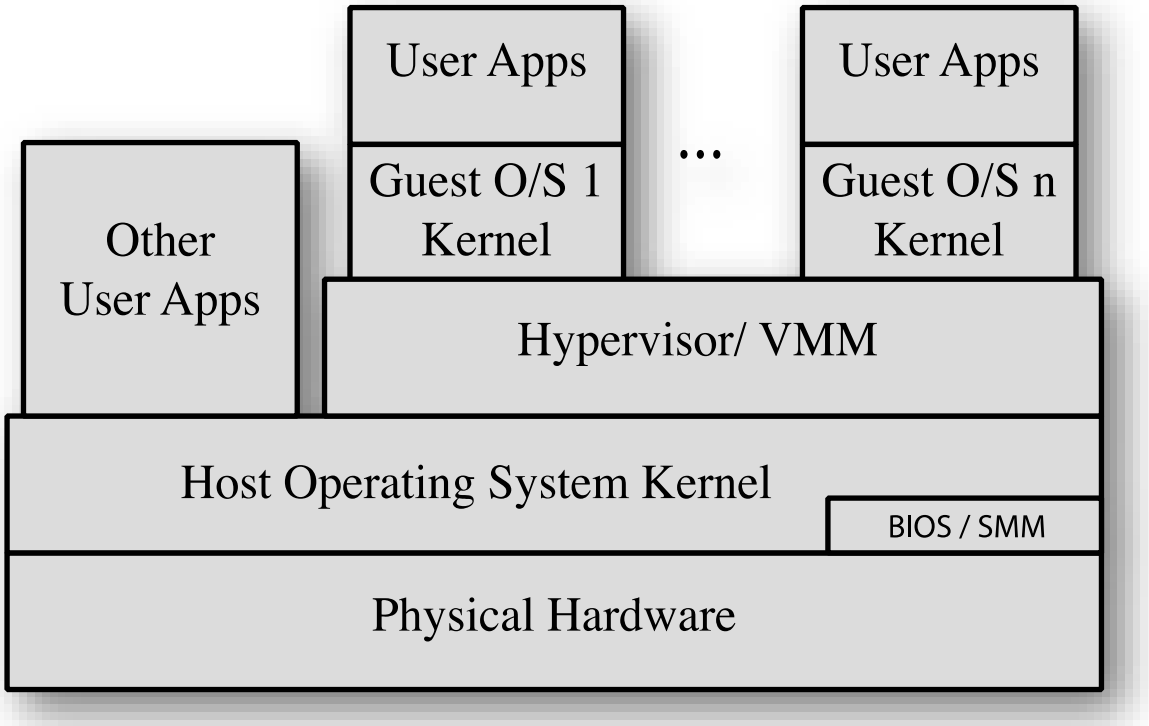
FANSHAWE

Type 1 - Bare-Metal Hypervisor



- A Bare-Metal Hypervisor system does not require another operating system

Type 2 - Host-Based Virtualization



- Host OS
  - Windows, Linux, OSX
- Hypervisor
  - VMware Workstation, VMware Fusion

Benefits of Virtualization

- Helps utilize the full capability of a server
  - Vendors may not want other applications running on the same physical server as their software as it may cause performance degradation
- Reduces management/support time, power consumption, etc.
- Can be easier to copy VMs and move them to other physical machines (more portable)

FANSHAWE

Benefits of Virtualization

- Assists with return on investment (ROI)
  - You can fit numerous virtual servers on one physical machine and only expand when overall physical computing power needs to be upgraded
- Reduces costs of the environment
  - Less rack space required
  - Less maintenance contracts
  - Improves disaster recovery

FANSHAWE

Hardware Resources & Virtualization

- Available hardware resources must be appropriately shared between the various guest Oss
  - CPU
  - Memory
  - Disk Space
  - Network Cards / Configuration
  - Any other attached devices

FANSHAWE

VMWare Workstation Terminology

Host – The physical computer you install VMware Workstation on is called the host computer, and its operating system is the host operating system.

Guest – The operating system running inside a virtual machine is called the guest operating system.

Note: During labs make sure you are aware of whether you are doing something on the host or guest OS.

FANSHAWE

Preserving VM States

- There are a variety of ways to preserve your guest operating system's state, providing you with a recovery path
- Snapshots
  - Taking an image of the VM at a specific point in time
    - After_Lab-01, After_Lab-02, etc.
- Suspend / Resume
  - Kind of like pause and play
- Cloning
  - Creating an entirely new VM

FANSHAWE

VM Encapsulation

- The ability to preserve the state of VMs is made possible because of the concept of VM Encapsulation
- VMs exist on the host machine as a set of files
- When you are taking a snapshot, or cloning a VM, you are preserving the current state of the files that describe the VM

FANSHAWE

Snapshots

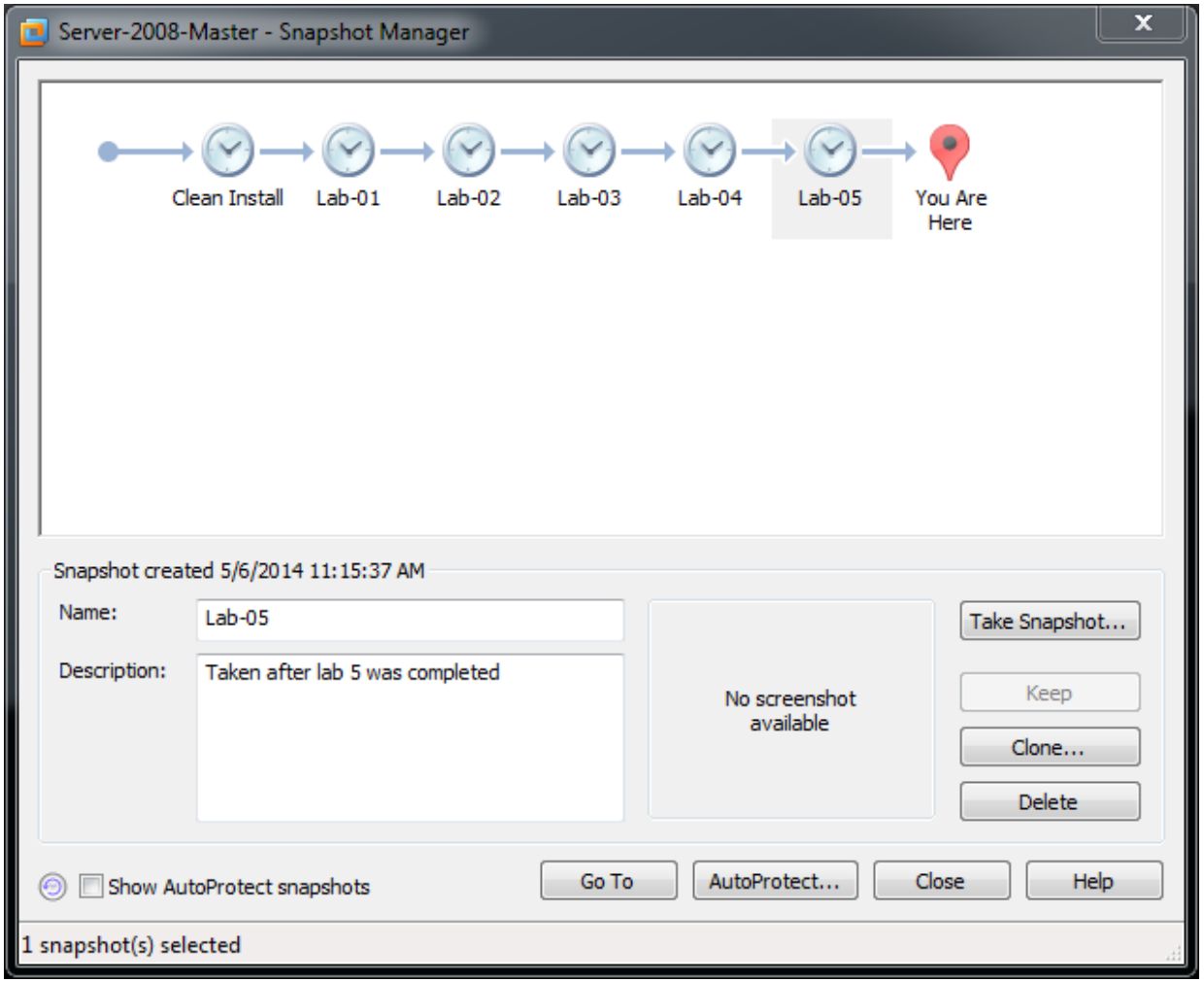
- Snapshots preserve the VM state so that you can return to the same state repeatedly
  - Very useful when testing the effects of malware and viruses
  - Can also be useful if you want to do a lab again when you are studying
- Information captured in a snapshot
  - Memory State: Contents of the virtual machine memory
  - Settings State: Virtual machine settings
  - Disk State: State of all the virtual disks

FANSHAWE

Types of Snapshots

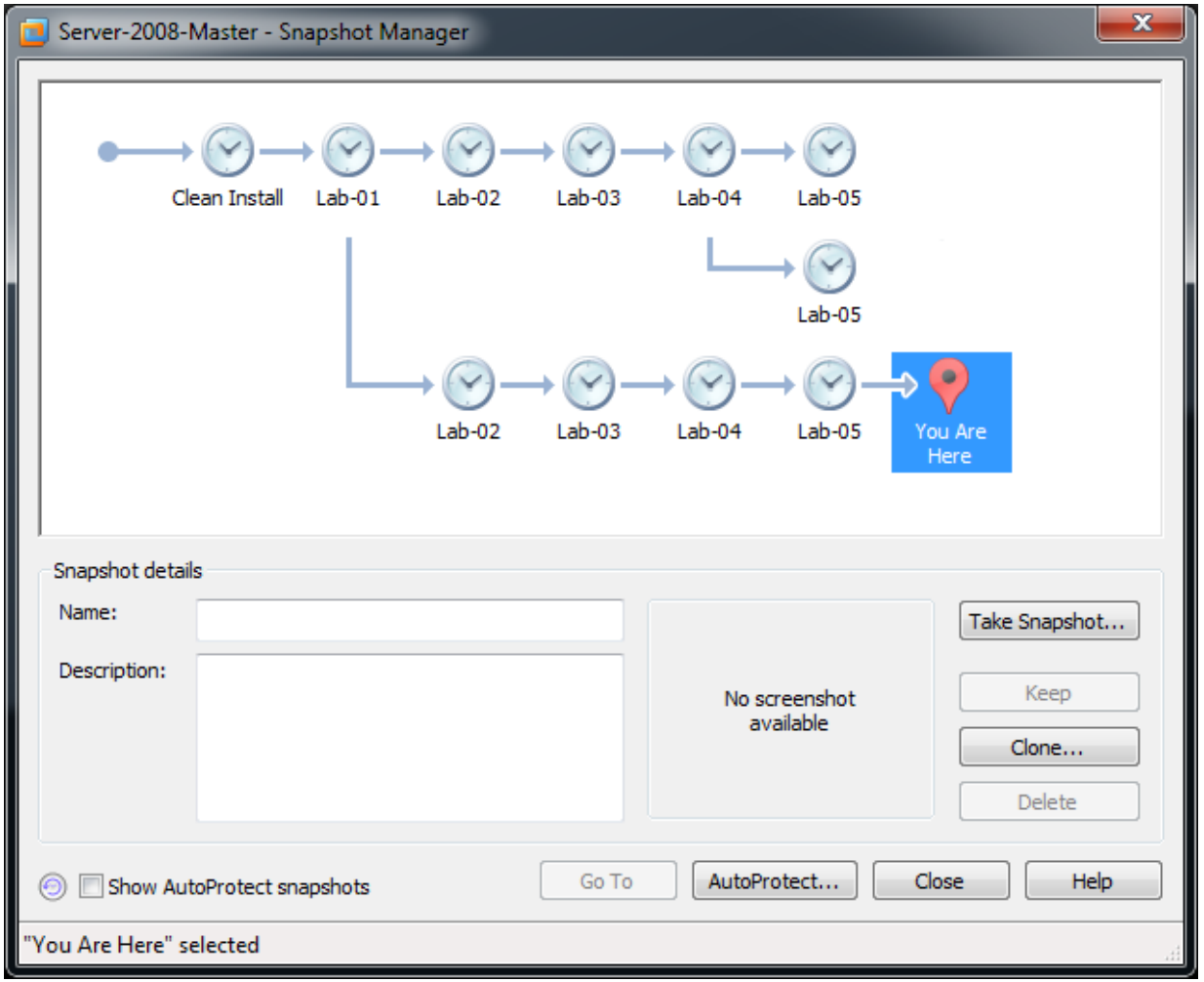
- Snapshots are taken in two ways:
- Linear
  - Take a snapshot and continue to use the VM from that point
  - Can restore to any point along the line
  - Supports over 100 snapshots
- Process Tree
  - Multiple Nested snapshots
  - Supports over 100 snapshots per branch
  - This is the model used when you are using snapshots to do your labs again when studying

Linear Snapshots



FANSHAWE

Process Tree Snapshots



FANSHAWE

VMWare Tools

- There is a lot of Host to Guest OS integration available when you are using Workstation
  - Copy/Paste
  - Drag/Drop
  - Shared Folders from the Host Machine
- VMware tools must be installed to use these features
- Every version of Workstation comes with a specific version of VMware Tools
- To ensure your VMs work properly you need to make sure you are using the correct version of VMware Workstation and Tools

Virtual Network Interface Cards (NIC)

- Several alternatives exist for providing network access
  - The guest OS may have direct access to distinct network interface cards on the system
  - The hypervisor may mediate access to shared interfaces
  - The hypervisor may implement virtual network interface cards for each guest, routing traffic between guests as required
- This last approach is quite common, and arguably the most efficient since traffic between guests does not need to be relayed via external network links

FANSHAWE

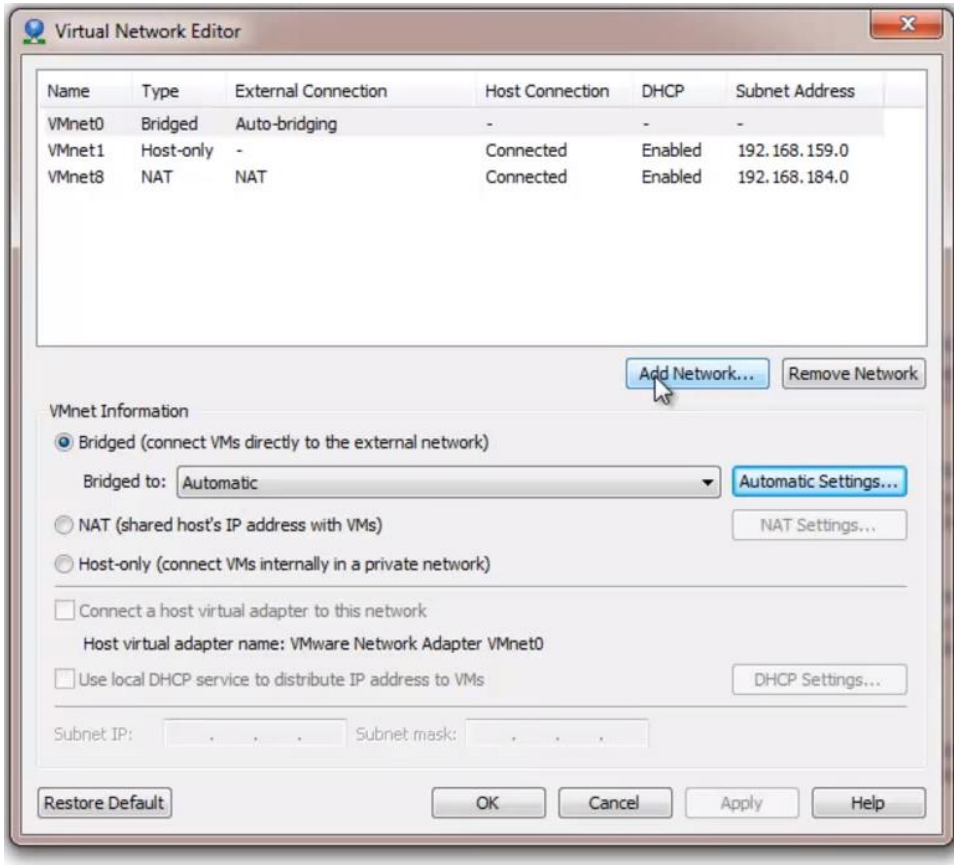
Virtual Switches

Network Type	Switch Name	DHCP
Bridged	VMnet0	No
NAT	VMnet8	Yes
Host-only	VMnet1	Yes

- Can be viewed through the Virtual Network Editor
- By Default there are three network types
  - Bridged
  - NAT
  - Host-Only

Default Network Types

- Clean Installation of VMWare Workstation

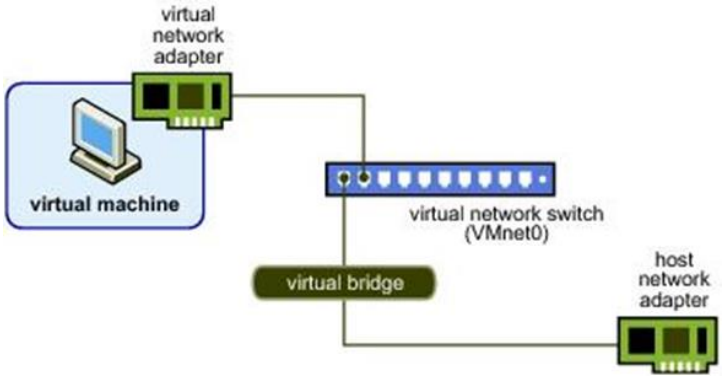


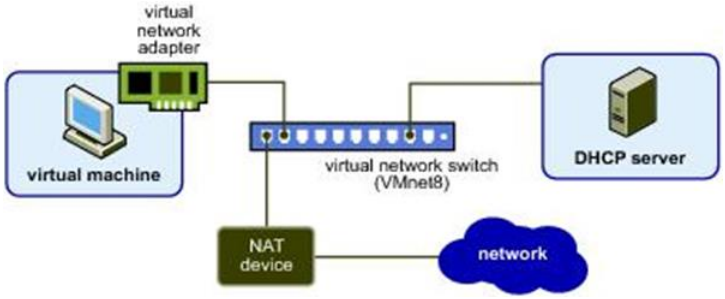
FANSHAWE

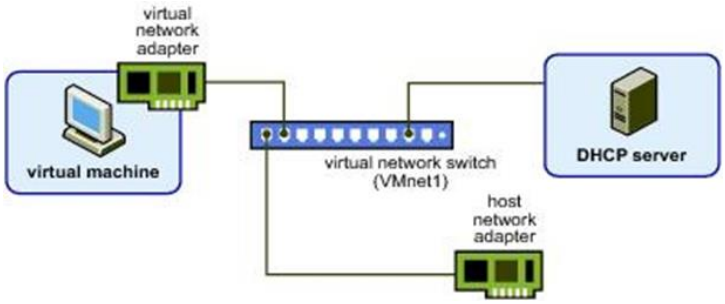
Adding Network Types

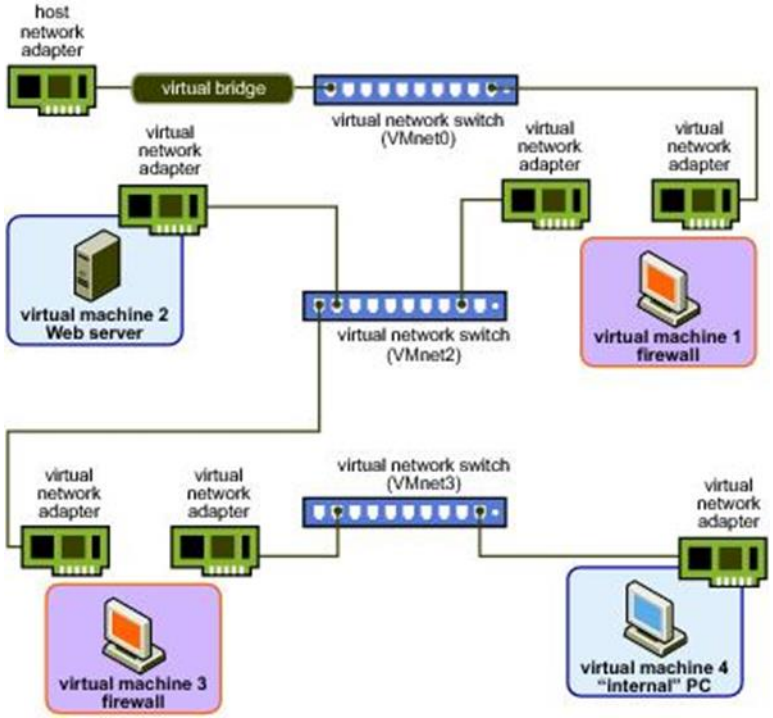
- In addition to the default network types on VMWare Workstation, you can add custom network types
- This is done in the Virtual Network Editor
- You will be creating these throughout the different courses in ISM
- Different Virtual Networks can communicate through virtual routers or multi-homed systems that utilize multiple NICs

Virtual Network Switches



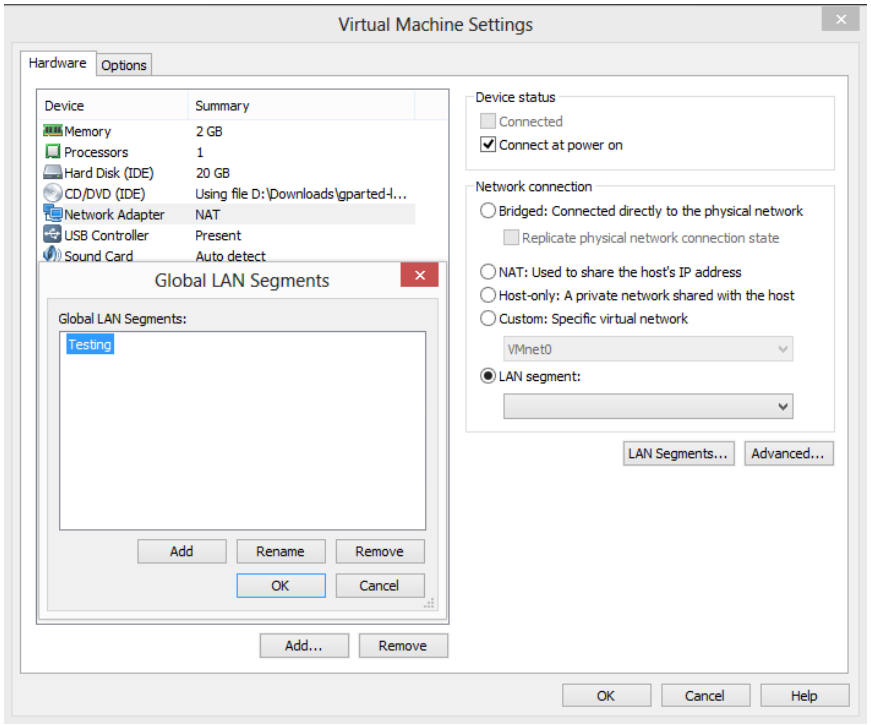






LAN Segments

- Provide complete isolation of VMs from host
- Inaccessible/Undetectable from other networks



FANSHAWE

LAN Segments

- Very good for testing environments
- Can be used to test the behavior of various types of Malware
- Sandbox environment ensures that contact to the outside (internet) is blocked
- May assist with determining what was compromised during an attack

FANSHAWE

LAN Segments

- Can also be a great way to test software updates for the O/S or other Applications prior to releasing them onto the production environment
- Allows for simulating a production environment in a lab setting with multiple machines on the same network
- Works with other virtualized test environments such as GNS3

FANSHAWE

Virtual Network Details

- Bridged
  - Connected to your laptops physical NIC
  - No isolation
  - VMware doesn’t provide DHCP
- Host Only
  - Connected to virtual NIC on laptop
  - Isolated from the Internet
  - VMware provides DHCP
  - VMs on network can talk to each other and host computer

FANSHAWE

Virtual Network Details

- Custom vmnet (most similar to host-only)
  - Connected to virtual NIC on laptop
    - Created when you create the custom vmnet
  - Isolated from the Internet
  - VMware provides DHCP
  - VMs on network can talk to each other and host computer
- LAN Segment
  - No virtual NIC on laptop
  - Completed isolated from laptop
  - VMware doesn’t provide DHCP

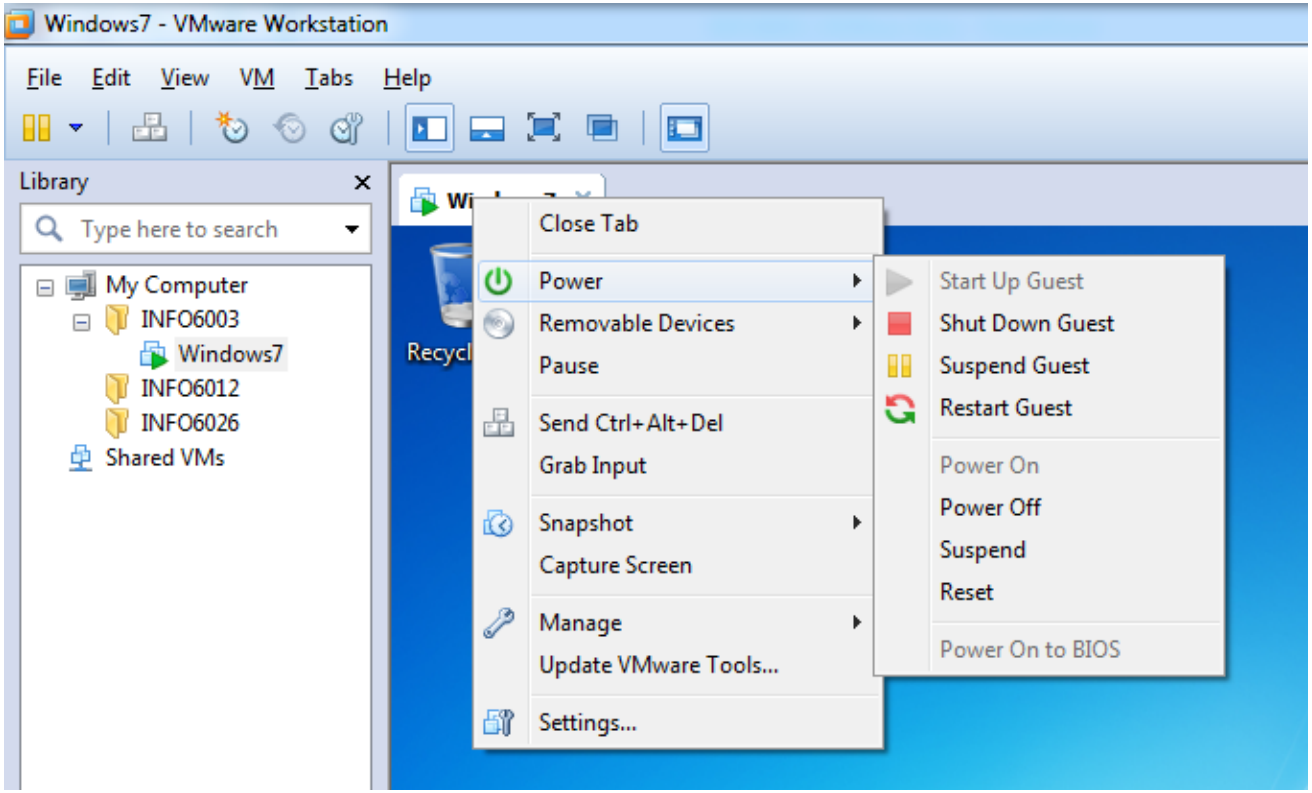
FANSHAWE

Virtual Network Details

- NAT
  - Connected to a virtual NIC on laptop
  - Internet connectivity
  - VMware provides DHCP
  - VMs on network can talk to each other, host computer and the Internet

Important Concept

- Powering Off is not the same as Shutting Down
- Always choose to shut your VMs down



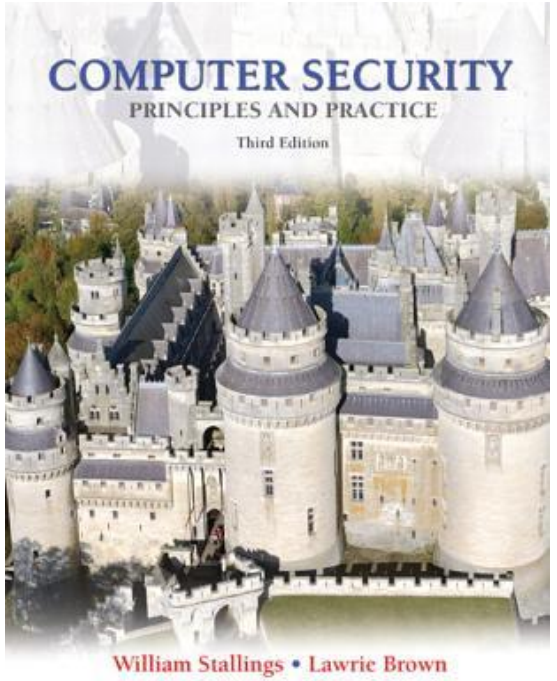
FANSHAWE

Matching Directory Structures

- You will all create an ISM folder within which you will store your VM and Lab related files:
  - Zipped VM images
  - Extracted VMs
    - A specific folder for each class
  - Install files
  - Screen Captures
- Keeping your files in this directory structure saves time later
  - You will have many copies of the same VM for different courses

Homework

- Read Chapter 1 for a general overview
  - Set Book: 3rd Ed. Computer Security - Principals and Practice by Stallings.
  - ISBN: 10:0133773922
  - ISBN: 13:9780133773927



Lab 00 - Setup

FANSHAWE

Initial Lab Setup

- Setup folder structure on your hard drives
- Install VMware Workstation 15
- Setup logical folder structure in Vmware that matches physical folder structure on hard drive
- Install 7Zip, all VMs were compressed with 7Zip
- Download and extract three zipped VMs from the College's FTP server
- Confirm functionality