UNIVERSITY OF AGDER

University of Nebraska Omaha

IT Administration Project University of Agder and University of Nebraska at Omaha

Illustration: Using Virtual Machines in CIST-4370; S. Nugen; 20110509

Slide 1

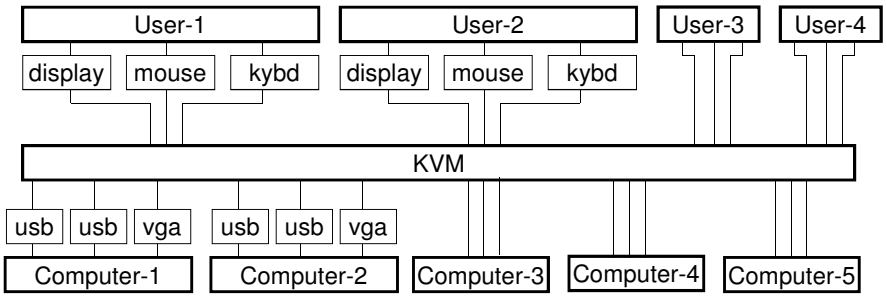
Context

- Illustrating the last lab assignment in CIST-4370 (Security Administration Using Windows)
  - Necessarily short since done in-class during "dead week" (the week before final exams)
  - Each student uses three Virtual Machines running on a single host to experiment with different security settings
    - VM1: Domain controller (result of an earlier lab) with Active Directory , DNS, and IIS (just for lab!)
      - Also contains a batch script solution for an earlier assignment so that students can interact with it... creates and deletes domain user accounts from values in a .CSV file
    - WC21: Windows client joined to the domain
    - HA70: Windows client not joined to the domain

Slide 2

STEAL Pods and KVMs

- In the IA lab environment (STEAL), student seats and hosts organized into where each pod includes:
  - Four seats
  - Five hosts
  - KVMs which interconnect Monitors, Keyboards, and Mice to one of five hosts



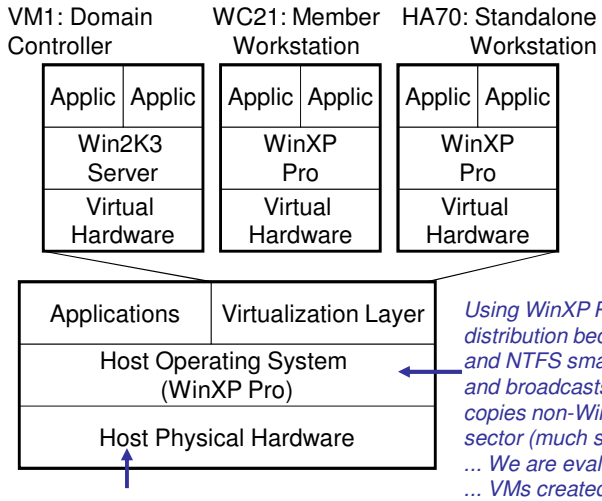
Slide 3

STEAL Pods and KVMs

- For all of the CIST-4370 Assignments, each student connects (through KVM) to a single physical host which runs
  - Host Operating System
  - VMWare Infrastructure (usually VMWare Workstation)
  - 1-3 Virtual Machines (VMs) running Guest Operating Systems
  - Host-only networking
- Thus, Pods and KVMs infrastructure is irrelevant

Slide 4

Three VMs for this Assignment



Planning to migrate course to using Windows Server 2008 with Windows 7 clients in Spring 2012

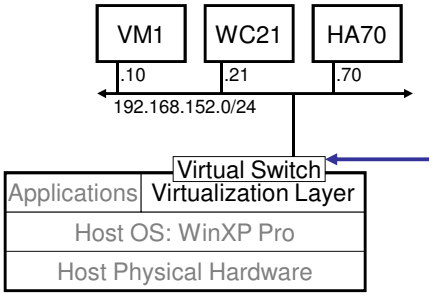
Using WinXP Pro instead of ESX or a Linux distribution because GhostCast handles FAT and NTFS smartly with respect to compression and broadcasts... GhostCast we're using copies non-Windows partitions sector by sector (much slower)
... We are evaluating alternatives to GhostCast
... VMs created with disk where the space is not preallocated... makes them much faster to upload and download (<3GB for Server)

Current host machines are dual core with 2GB DDR2 RAM

Slide 5

Host-Only Networking

- Self-contained, Non-interfering
  - All the VMs interconnected on same virtual subnet through infrastructure-provided virtual switch
  - No routing in the Host Operating System, so VMs interconnected in each host isolated from all the VMs running in other hosts... Thus, students don't interfere with each others' Windows and DNS domains



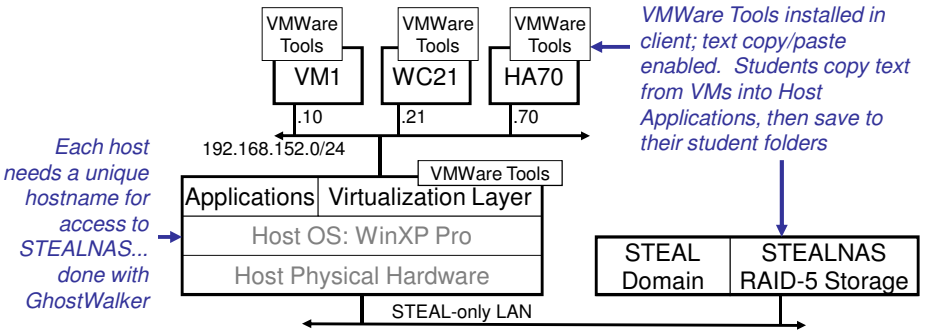
Switch really acts like a shared domain Ethernet hub. Thus network traffic can be sniffed by tools like Wireshark executing on the Host O/S or any of the VMs.

This design does not depend on VMWare... we have also used VirtualBox with Host-Only networking.

Slide 6

Host-Only Networking cont'd

- Students like to save and submit their work...
  - VMs are not guaranteed to persist across student sessions
  - VMs themselves too large for 28 students to simultaneously save them to student folders



Slide 7

Lab Objectives

- Examine Windows Firewall settings, particularly the exceptions
- From WC21, try to change the contents of a folder shared by VM1
  - Fails because share permissions do not permit
- From WC21, connect to Administrative Share C$ on VM1
  - net use command
  - Now able to change the contents of the folder shared by VM1 because share permissions not relevant

Slide 8

Lab Objectives cont'd

- From HA70, use the same commands used on WC21 to connect to \\VM1\C$... change the content of C:\Inetpub\wwwroot\default.html
  - Key point: HA70 is not a managed member of the domain
- Use scanning tools on HA70 to scan VM1
  - nmap
  - SuperScan
    - Different results when the scan type is changed from SYN to Connect
    - Enumerate Windows services using different options

Slide 9

Lab Objectives cont'd

- Update domain security policy for more auditing
  - Make the Group Policy changes on VM1
  - Apply them to WC21
  - Use HA70 to access WC21 (e.g., net use command)
  - Verify remote connection requests now being logged on WC21 Event Logs
- On HA70, run a simple batch script that writes a simple batch script which does a simple brute-force attack against WC21

Slide 10

Lab Objectives cont'd

- On HA70, use psexec command to remotely execute a command shell on WC21 where StdIn and StdOut are redirected back to HA70
  - Key point: No need to preinstall psexec on the machine being remotely controlled
- Change the firewall on WC21 to prevent remote control via psexec
  - Key point: Breaks file sharing

Slide 11

Lab Objectives cont'd

- Use .reg files to prevent (or reenable) the automatic creation of administrative file shares like C$
  - Key point: .Reg files an alternative to Group Policy
  - Key point: Disabling administrative shares does not interfere with psexec as it can make use of IPC$
- Disable all protocols except for TCP/IP from WC21 network adapters
  - What impact on the result of running port scans?
  - What impact on psexec?

Slide 12

Lab Objectives cont'd

- Disable services on VM1 and WC21
  - What impact on the result of running port scans?
  - What impact on the result of running netstat -ano from within VM1 and WC21?

Slide 13