Cyber Security Education
Consortium (CSEC)

Ken Dewey
Cyber Security
Rose State College
Midwest City, OK
Rose State College

Making the move from physical to virtual
Equipment

• The Rack
Equipment cont.

- More Rack
Equipment cont.

- Rack, inside front
Equipment cont.

- Rack, inside front (workstation,
Equipment cont.

- Rack, inside back (network)
Equipment cont.

- Rack, inside back (domain controllers)
• Rack, inside back (core switch)
Equipment cont.

Rack, inside back (ESX Hosts)
Hardware

• 2 Dell R710 servers running ESX 4.1
  – 96 GB RAM
  – Dual Quad Core Intel Xeon @ 3.20 GHz
  – 2 TB Local storage (not used)

• 1 Dell EqualLogic PS6000 series SAN
  – 9.6 TB storage (6.3 TB in Volume)
  – 16 drives (1 redundant, 1 spare)
  – RAID 50 (striping with distributed parity)
Hardware cont.

- SAN Management (Drive with X is
Network

• 10 MB asynchronous line (donated by OneNet)
  – Backbone for virtual systems
  – Current utilization less than 5%
• Two Cisco 2800 routers
  – virtual network routed through OneNet
  – Everything else routed through Cox
• Dell PowerConnect 6224 switch
  – 24 ports, all used
  – Additional switch ordered
Network

• Currently configured on a 10.10.X.X Class B subnet
• Infrastructure currently running on 10.10.0.X subnet
• Student hosts currently running on 10.10.50.X subnet
• Ideal for assigning different scanning projects. Students can scan large network segments without affecting other hosts.
Network cont.

- MRTG showing network utilization over past month

`Monthly' Graph (2 Hour Average)

<table>
<thead>
<tr>
<th></th>
<th>Max</th>
<th>Average</th>
<th>Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>In</td>
<td>13.6 kB/s (0.1%)</td>
<td>1706.0 B/s (0.0%)</td>
<td>138.0 B/s (0.0%)</td>
</tr>
<tr>
<td>Out</td>
<td>194.3 kB/s (1.6%)</td>
<td>20.1 kB/s (0.2%)</td>
<td>87.0 B/s (0.0%)</td>
</tr>
</tbody>
</table>
Software

- ESX hosts running ESX 4.1
  - Linux based hypervisor
- vCenter server running Win Server ‘08 R2
  - allows aggregation of disparate ESX hosts
  - Central point of management
- Database server running Win Server ‘08 R2
  - Current RDBMS is SQL Server 2008
  - Current size is 375 MB
Software cont.

- vSphere client
  - Allows interaction with ESX hosts and their virtual machines
  - Interfaces with Active Directory for user management
  - Allows creation of roles and privileges
  - Once vCenter is installed, all management is done in vSphere through the vCenter host
vSphere Client

To directly manage a single host, enter the IP address or host name. To manage multiple hosts, enter the IP address or name of a vCenter Server.

IP address/Name: vc.cyber.rose.edu
User name: 
Password: 

Use Windows session credentials

Login Close Help
vSphere Client
vSphere Client
vSphere Client

- Multiple OS’s simultaneously
Extensibility

- vCenter/vSphere approach manages expansion extremely well
- New ESX hosts only need to have the ESX software installed and an IP address assigned
- They are then added to the cluster through the vSphere client
- Storage space expansion via SAN works the same way
Upgrades

• ESX host designed to support 25-40 virtual machines
• Currently have approximately 150 machines
• Experiencing slight hardware bottleneck
• Ordered two additional R610 servers
  – Same specs as 710s except only 150GB local storage
  – Will solve hardware problem