Virtual Lab Environment
Introduction Slide

- Virtual Lab Environment
- Network Topography
- Virtual Forensic Workstations
Virtual Lab Environment

**Advantages:**
- Templates for New Cases
- Archiving of VMs
- Replacement Costs of Physical Machines
- Remote Logins
  - Two-Factor Authentication

**Disadvantages:**
- Lack of “hands on feel”
- Initial Overhead Costs
- Requires Dedicated Personnel
Network Topography

- Corporate Network / VPN Layer
- Forensic Lab Layer
- Storage Layer
Network Topography

- Corporate Network / VPN
- IT Network
- Forensic Lab Network
- Storage Network
  - NAS 0
  - NAS 1
Network Topography

Corporate Network / VPN

IT Network

Forensic Lab Network

Cluster 0

Cluster 1

Cluster 2
CLUSTER 0

- Authentication Server
  - OpenLDAP
  - RADIUS
- Admin Server
  - AV Updater
  - Web Portal
- Admin Workstation
  - XenConsole
- License Server
  - FTK
  - EnCase
- Storage Firewall

SPECIFICATIONS

- VMWare ESX
  - For USB Pass Through
- 1 Physical Machine
Network Topography

CLUSTER 1
- Xen License Server
- Web Provisioning
- Analysis VMs

SPECIFICATIONS
- XenServer Enterprise
  - Scalability
- 2 Physical Machines
  - Server Apps
    - 24 GB RAM
    - 1x Xeon
  - Analysis VMs
    - 512 GB RAM
    - Quad Xeon (40 CPU)
CLUSTER 2

- FTK Infrastructure
  - PostgreSQL Database
  - Worker0
  - Worker1
  - Worker2
  - Worker3

SPECIFICATIONS

- XenServer
- 2 Physical Machines
Network Topography

Forensic Lab Network

Cluster 0
Cluster 1
Cluster 2

Storage Network

NAS 0
Environments

NAS 1
Evidence
Virtual Forensic Workstations

- **XenCenter**
  - Windows 7 Workstations
    - Template
    - Updates in SVN
    - Access via RDP
  - Ubuntu 10 Workstations
    - Template
    - CLI
    - Access via SSH
Virtual Forensic Workstations

[Image: Screenshot of XenCenter showing HQ Forensic Lab - Cluster 1 with various virtual machines and folders such as CentOS 6.0 (64-bit) (experimental), Citrix License Server Virtual Appliance, DVS Controller 8124 amd64, XenServer 6.0 Evaluation License Server Virtual Appliance, DVD drives, Local storage, Removable storage, GM-Ubuntu Maverick Meerkat 10.10 (64-bit) Environment 02-21-2012 (old), GM-Ubuntu Maverick Meerkat 10.10 (64-bit) Environment 06-12-2012, GM-Win7 Environment pGina 03-23-2012 (old), GM-Win7 Environment pGina 05-29-2012, DVD drives, environments, NFS ISO library, Removable storage, GM-Ubuntu Maverick Meerkat 10.10 (64-bit) Environment 06-12-2012 Template, GM-Win7 Environment pGina 05-29-2012 Template, OLD GM-Ubuntu Maverick Meerkat 10.10 (64-bit) Environment 02-21-2012 Template, OLD GM-Win7 Environment pGina 03-23-2012 Template, HQ FTK - Cluster 2]
Virtual Lab Environment