Evolution of the ASSERT Computer Security Lab

Brian Hay
Kara Nance
University of Alaska Fairbanks

Agenda

- Motivation
- Initial Configuration
- Virtualization – Host Based Images
- Virtualization – Network Based Images
- Network Isolation
- Alternative Approaches

Motivation

- Need for an environment which allows students, faculty, and staff to gain hands-on experience with IA concepts.
- Need for a controlled research environment.
- General purpose labs are typically ill-suited for this use.

Needs

…so you want to build a lab…

- Space
- Equipment
- Champion

Proof of Concept Lab

- General purpose CS lab moved to Windows/Linux dual boot, freeing some space for a dedicated IA Lab.
- However, there was little funding available for lab equipment.

So, we looked for alternate sources of equipment!

Surplus Equipment

- Many institutions maintain a surplus warehouse.
  - Good source of older, but still useful, equipment.
  - For example, 30 identical 1GB hard drives (computer forensics exercises).
  - Extra NICs and RAM.
- Lab upgrades were also a good source of multiple identical computers.

Surplus Equipment

- Initial configuration
  - 10 homogenous systems (surplus)
  - 1 "server" with extra HDD (surplus)
  - 10 monitors (surplus)
  - Basic switch (~$50)
  - Ethernet Cable (~$50)

Initial Configuration

- Workstations
  - 20 GB HDD split into four 5GB partitions.
  - Different OS loaded on each partition (2 Windows, 2 Linux).
  - Base images stored on server.
  - Script allows user to reload any partition with base image.
- Server
  - DHCP, DNS, Web, Mail, and base images.

Initial Configuration

- Advantages
  - Gives user full control of system.
  - Ability to restore base configuration.
  - Lots of basic IA exercises possible.
- Disadvantages
  - Not easy to save configurations.
  - Limited network configurations.
  - User tied to particular workstation.
  - Only one system per physical machine.

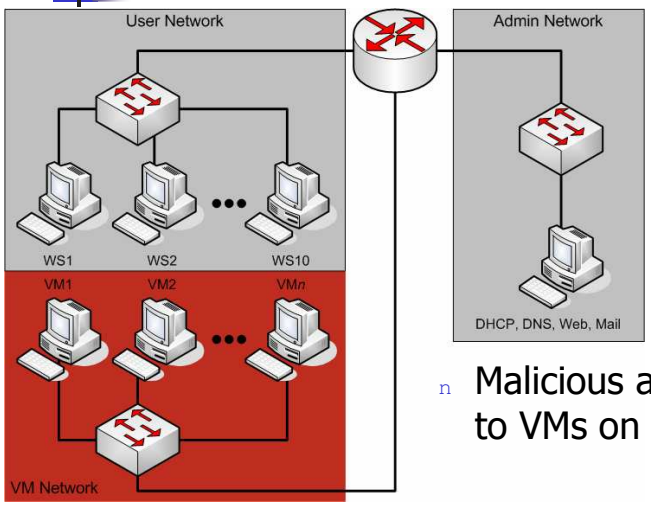
Initial Configuration

- Major Advantage
  - Proof-of-concept lab was used to generate momentum
    - Credibility
    - Fundability
    - Excitement

Virtualization – Host Based Images

- NSF Capacity Building grant and UAF Technology Advisory Board provided some funds for new equipment.
  - Workstations with more RAM and larger HDD to support virtualization.
  - Network equipment – router and managed switch.
  - VMware workstation software.

Virtualization – Host Based Images



- Malicious activity confined to VMs on VM network.

Virtualization – Host Based Images

- Advantages
  - Gives user full control of VMs.
  - Ability to snapshot (save) and restore VM configuration.
  - Multiple VMs per physical machine (and use of virtual networks).
- Disadvantages
  - Limited network configurations.
  - User tied to particular workstation.

Virtualization – Host Based Images

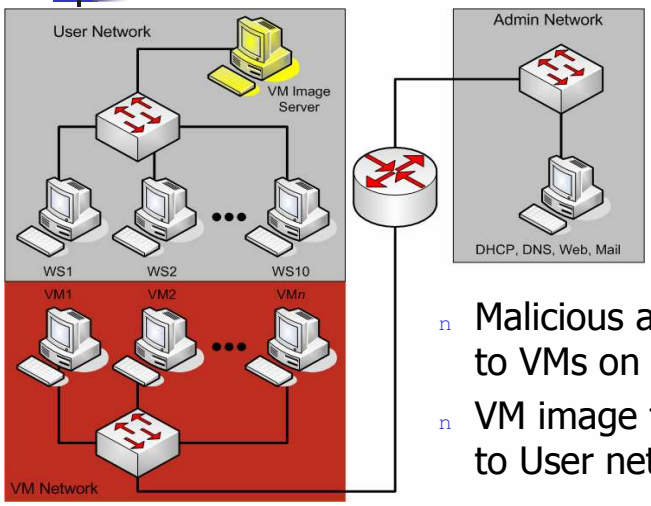
- Major Advantage

  Generated further momentum
  - More credibility
  - More fundability
  - More excitement

Virtualization – Network Based Images

- UAF internal grant provided some funds for new equipment.
  - Server with additional storage (~1.5TB).
- VM Images moved from individual workstations to server.

Virtualization – Network Based Images

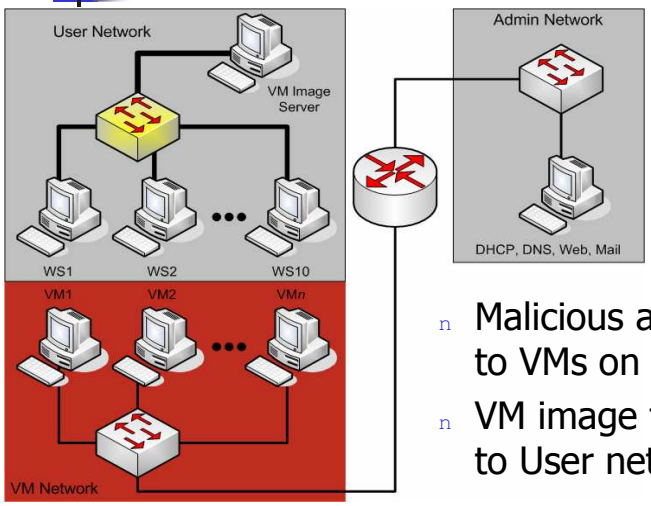


- Malicious activity confined to VMs on VM network.
- VM image traffic confined to User network.

Virtualization – Network Based Images

- Network determined to be performance limiting factor.
- Replaced 100Mb user switch with Gigabit switch.
  - Workstations had existing Gigabit NIC.
  - 3Gb/s bonded channel from server to switch.
  - 1 Gb/s link to each workstation.

Virtualization – Network Based Images



- Malicious activity confined to VMs on VM network.
- VM image traffic confined to User network.

Virtualization – Network Based Images

- Advantages
  - Gives user full control of VMs.
  - Ability snapshot (save) and restore VM configuration.
  - Multiple VMs per physical machine (and use of virtual networks).
  - User no longer tied to particular workstation.
  - Improved VM performance (no lag during normal use, and acceptable performance during start/stop/snapshot operations).
- Disadvantages
  - User required to physically be in ASSERT Lab.

External Network Connectivity

- ASSERT Lab is physically isolated from external networks.
  - Makes updating/patching and new software installation more challenging.
  - However, no opportunity for accidental impact on external networks.

Alternate Configurations

- Boot existing general purpose lab system with:
  - Live CD
    - Limited ability to save current state.
    - User can easily compromise physical system.
  - Alternate partition
    - User tied to physical machine.
    - User can easily compromise physical system.

Conclusions

- Extended to Montana State University
- Continually evolving
- NSF Planning Grant
- Research Partnerships