



ASSERT Computer Lab

Brian Hay
University of Alaska Fairbanks



Agenda

- n Motivation
- n Initial Configuration
- n Virtualization – Host Based Images
- n Virtualization – Network Based Images
- n Network Isolation



Motivation

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



Proof of Concept Lab

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



So, we looked for alternate sources of equipment!

Surplus Equipment

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



Surplus Equipment

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



Initial Configuration

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



Initial Configuration

n Advantages

- n Gives user full control of system.
- n Ability to restore base configuration.
- n Lots of basic IA exercises possible.

n Disadvantages

- n Not easy to save configurations.
- n Limited network configurations.
- n User tied to particular workstation.
- n Only one system per physical machine.



Initial Configuration

n Major Advantage

Proof-of-concept lab was used to generate momentum

- n Credibility
- n Fundability
- n Excitement

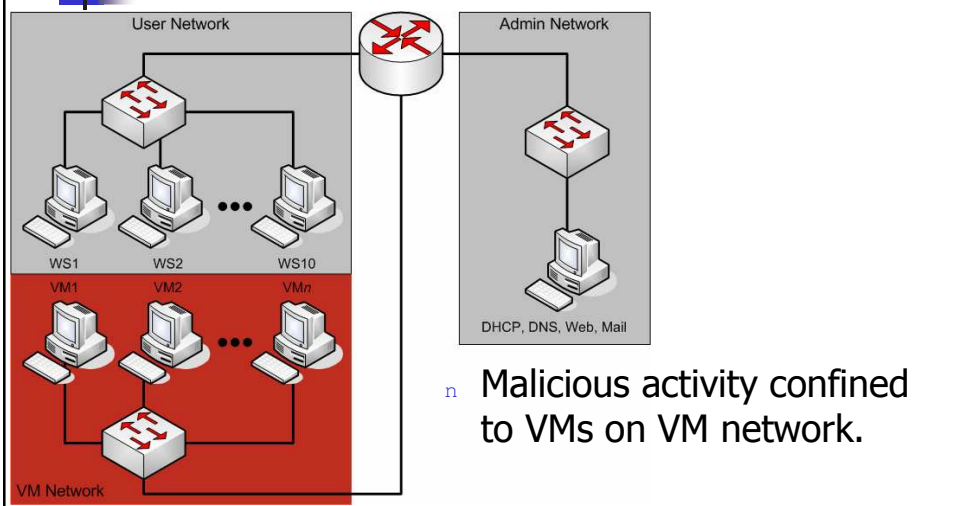


Virtualization – Host Based Images

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



Virtualization – Host Based Images



- n Malicious activity confined to VMs on VM network.



Virtualization – Host Based Images

n Advantages

- n Gives user full control of VMs.
- n Ability to snapshot (save) and restore VM configuration.
- n Multiple VMs per physical machine (and use of virtual networks).

n Disadvantages

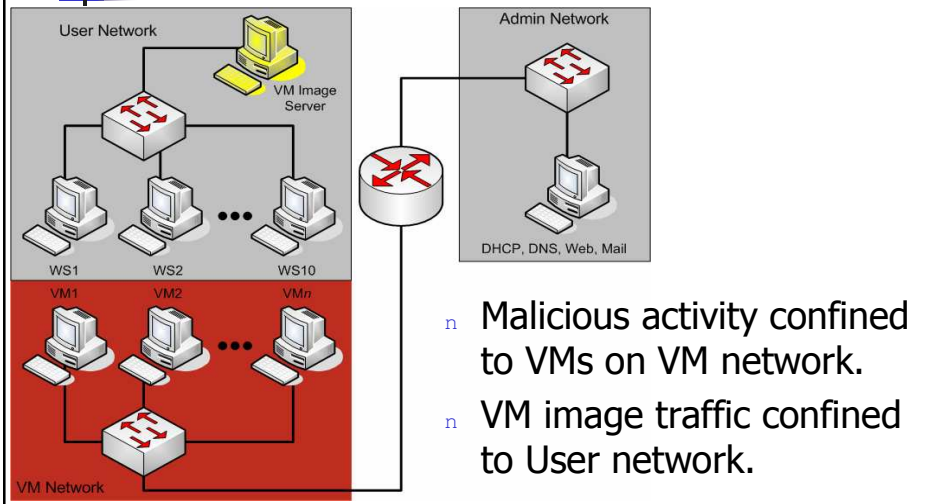
- n Limited network configurations.
- n User tied to particular workstation.



Virtualization – Network Based Images

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

Virtualization – Network Based Images



Virtualization – Network Based Images

n Advantages

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

n Disadvantages

- n User required to physically be in ASSERT Lab.



External Network Connectivity

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



External Network Connectivity

- n Currently developing network accessible lab environment.
 - n Access to VM interfaces available over network.
 - n VM traffic remains only on isolated network(s).
 - n Currently evaluating software/hardware options with test system.



Conclusions

- n Lab is continually evolving.
- n Excellent facility for testing, teaching, and researching computer/network security topics.
- n Network-accessible lab will allow for larger user population.