Using Virtualization to Improve Security

Jay Judkowitz
Product Manager, ESX Server
VMware, Inc.
This presentation may contain VMware confidential information.

Copyright © 2005 VMware, Inc. All rights reserved. All other marks and names mentioned herein may be trademarks of their respective companies.
Agenda

- Introduction
- Virtualization Introduction
- Game Changing Techniques
- Application Examples
- Q & A
VMware and Security

- Key personnel with rich security backgrounds in secure operating systems and applications
- Papers and books attributed in security to VMware employees
- Fundamental research projects with leading universities to further enhance the possibilities of security
- Internal processes including third-party source code audits, internal vulnerability assessment of code and recognized certifications (including Common Criteria by Q4 2005)
- Affiliations with various standards bodies to ensure we guide and adhere to industry set security standards
Agenda

- Introduction
- Virtualization Introduction
- Security Properties of Virtualization
- Application Examples
- Q & A
Security Challenges

- Must deal with larger and larger numbers of systems
- Keep up with regulatory and departmental policies
- Enforcing system uniformity across all servers and desktops
Virtualization Basics

Before Virtualization:
- Single OS image per machine
- Software and hardware tightly coupled
- Running multiple applications on same machine often creates conflict
- Underutilized resources
- Inflexible and costly infrastructure

After Virtualization:
- Break dependencies between OS and hardware
- Virtual machines are hardware-independent: they can be provisioned anywhere
- Manage OS and application as single unit by encapsulating them into virtual machines
Agenda

- Introduction
- Virtualization Introduction
- Game Changing Techniques
- Application Examples
- Q & A
Game Changing

Don’t defend, deflect.

- Isolation
- Attack Mitigation
- Policy Enforcement
- Defense-in-depth (cheaper)
- Encapsulation
Isolation

- *Don’t make your problems mine*
  - Virtual machine can be started/stopped/crashed without affecting other virtual machines and host system
  - Patches, configurations, and differing versions of software can be maintained throughout the network
  - Immediate virus containment

- *Abstraction from physical hardware*
  - Control access to hardware, including writeable devices (such as floppies, USB, etc...)
Isolation

- Keep data, network, or memory separate and secure.
- Maintain isolated security testing ground
- Honeypots
- Isolation of:
  - Memory
  - Network – virtual switches
Attack Mitigation

- Quicker quarantine of system or entire network
  - Turn off virtual switches/routers
  - Execute state change across multiple virtual machines at the same time (potentially entire network)
- Failure of single virtual machine does not affect physical host or other virtual machines
  - Robust DoS, DDoS protection possible
Attack Mitigation, cont.

- Recover quicker from attacks
  - Build new production system from saved clone (with merged changes)
  - Use ongoing snapshots (rollbacks) to automate recovery
- Create forensics copy for later review
  - Move production system back into service as quickly as possible
  - Create forensics copy for technical or legal review
Policy Enforcement

- Develop template virtual machine
  - Replicate policies and configurations
  - Enforce security configurations (including DRM)
  - Application specific templates (virtual machines for databases, for business applications, for security components, etc…)
Defense-in-Depth (Cheaper)

- Defense-in-depth
  - Each virtual machine can contain security protection (application firewall/endpoint security)
  - Firewall virtual machines (virtual firewalls) can be placed between virtual machines and/or subnets
  - Different security components/vendors can be quickly deployed
Agenda

- Introduction
- Virtualization Introduction
- Game Changing Techniques
- Application Examples
- Q & A
Monitor “health” of systems:

- Virus detected
- virtual machine isolated and crashes
- Virtual switch isolates virtual machine to prevent further damage
Policy Enforcement
Network Access Control

To maintain patch levels and antivirus signatures up-to-date:
- Virtual machines initially quarantined to host only network
- Virtual machines only allowed to connect to patch management and antivirus servers
- Virtual machines granted access to LAN if step 2 “passes”
Policy Enforcement
Network Access Control

To maintain patch levels and antivirus signatures up-to-date:
- Virtual machines initially quarantined to host only network
- Virtual machines only allowed to connect to patch management and antivirus servers
- Virtual machines granted access to LAN if step 2 “passes”
Policy Enforcement
Network Access Control

To maintain patch levels and antivirus signatures up-to-date:

- Virtual machines initially quarantined to host only network
- Virtual machines only allowed to connect to patch management and antivirus servers
- Virtual machines granted access to LAN if step 2 “passes”
Policy Enforcement
Network Access Control

To maintain patch levels and antivirus signatures up-to-date:
- Virtual machines initially quarantined to host only network
- Virtual machines only allowed to connect to patch management and antivirus servers
- Virtual machines granted access to LAN if step 2 “passes”
Agenda

- Introduction
- Virtualization Introduction
- Game Changing Techniques
- Application Examples
- Q & A
Questions?

Jay Judkowitz
jay@vmware.com