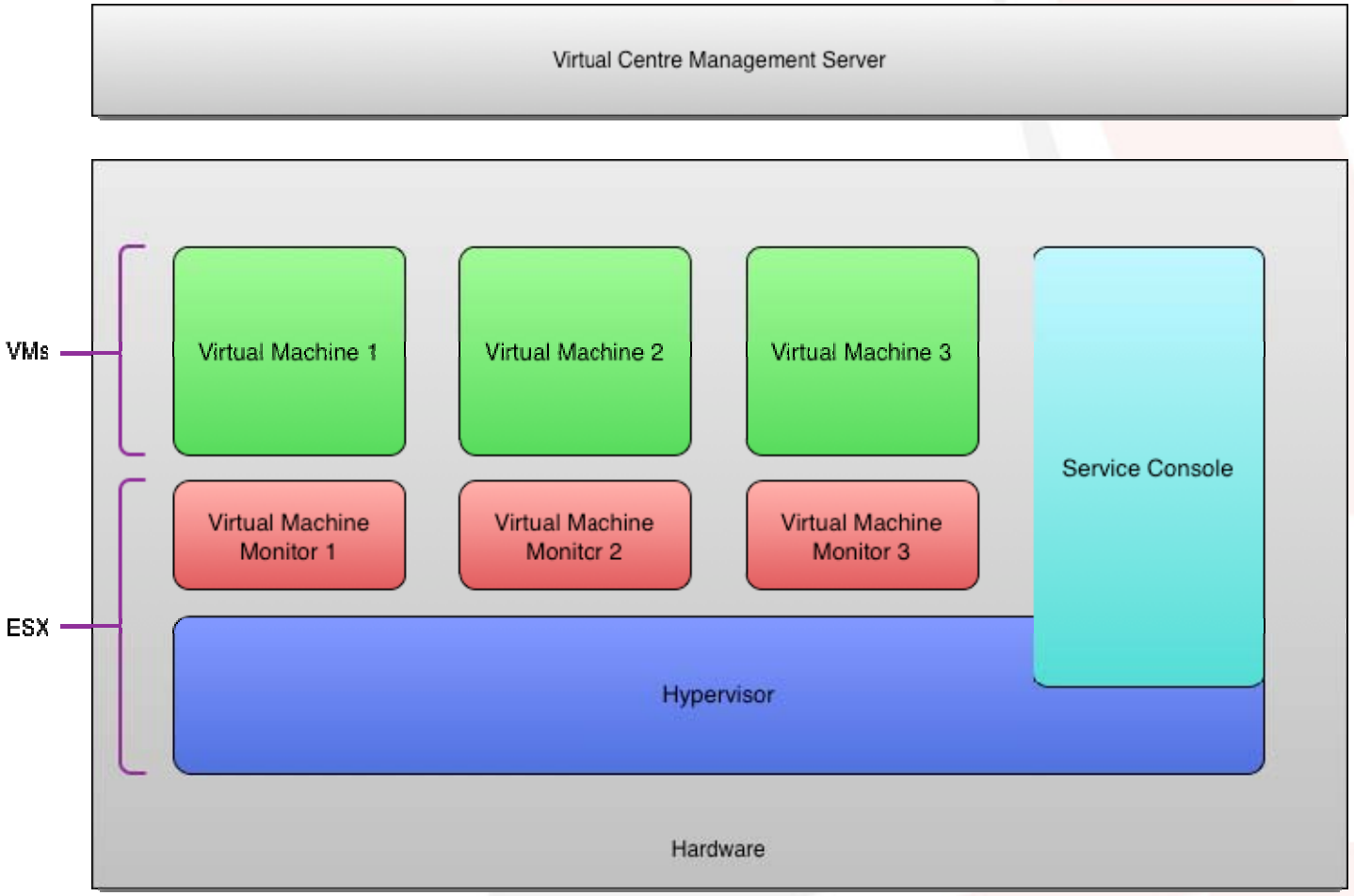
Virtualisation: Pitfalls in Corporate VMware Implementations

18 May ’09

Agenda

1. Technology overview
2. Typical corporate implementations
3. Common pitfalls and solutions
4. Conclusion

VMware ESX Software Architecture & Concepts



Other Concepts:

1. VMotion
2. Virtual Infrastructure Client
3. Remote Command Line Interface (RCLI)

Typical Corporate Implementations

- Why are they using virtualisation technology?
  - cost reductions, flexibility and efficiency, increase business resiliency
- What are organisations using VMware for?
  - test environment, production systems, virtual desktop, virtual appliances
- What are security practitioners using VMware for?
  - sandboxing, forensic analysis, and honeypotting
- What are organisations not virtualising?
  - CPU intensive apps
  - firewalls
- How are they using it?
  - simply, with little regard for security

Theoretical Security Problems and Hype

- Compromise the hypervisor, compromise every virtual machine!
- What about the Red Pill and the Blue Pill?

Vulnerabilities – Hosted Versions

- Most of the serious VMware issues (code execution on Host) identified to date are against the "Hosted" versions (Workstation, GSX, etc.).
  - e.g. CVE-2005-4459
    - Vulnerability was identified in VMware Workstation (and others) in the NAT component, which could be exploited by a malicious guest to execute arbitrary commands on the Host OS.
    - Patch made available by VMware.
  - e.g. CVE-2007-4496
    - Vulnerability was identified in VMware Workstation (and others) that could allow a guest operating system user with administrative privileges to cause memory corruption in a host process, and thus potentially execute arbitrary code on the host.
    - Patch made available by VMware.

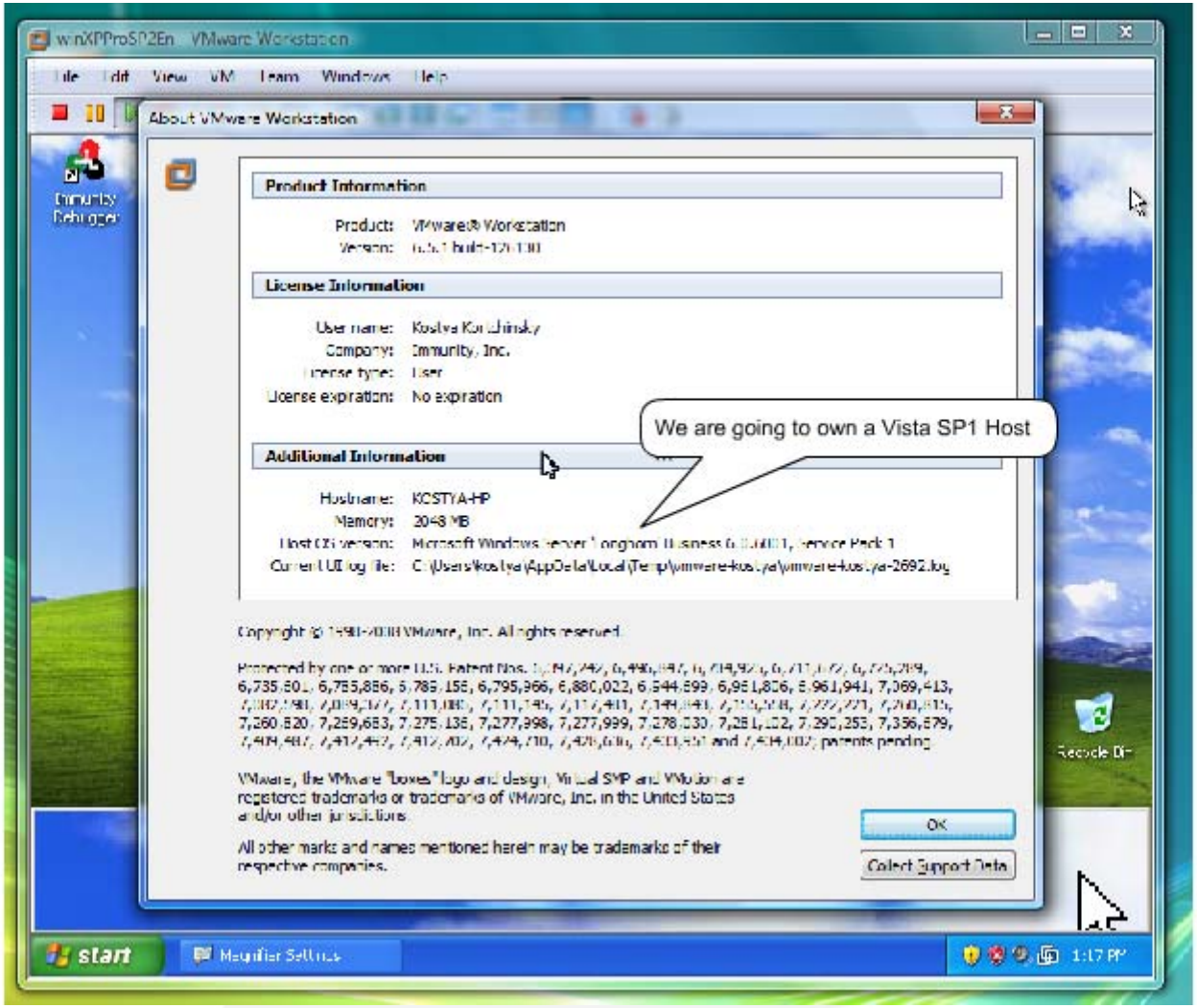
Vulnerabilities – Bare-metal Versions

- What about serious security issues with the enterprise "bare-metal" solution?
  - e.g. CVE-2009-1244 - VMSA-2009-0006 - (10 April 2009)
    - "A critical vulnerability in the virtual machine display function "might" allow a guest operating system to run code on the host."
    - Affects both VMware hosted and bare-metal solutions.
    - Patch made available by VMware.

- Further research found the following:
  - "By combining multiple indexing flaws in VMWare's usage of 3D context structures, [a user] is able to both leak from and write to physical host memory. It can do this in a reliable way from inside a virtual machine by combining SVGA framebuffer relative memory leaks with 3D context based write-to-memory flaws, effectively compromising any virtual 'air gap' between physical and virtual hardware."

    credit: Kostya Kortchinsky of Immunity Inc.

Exploit Demonstration - CVE-2009-1244

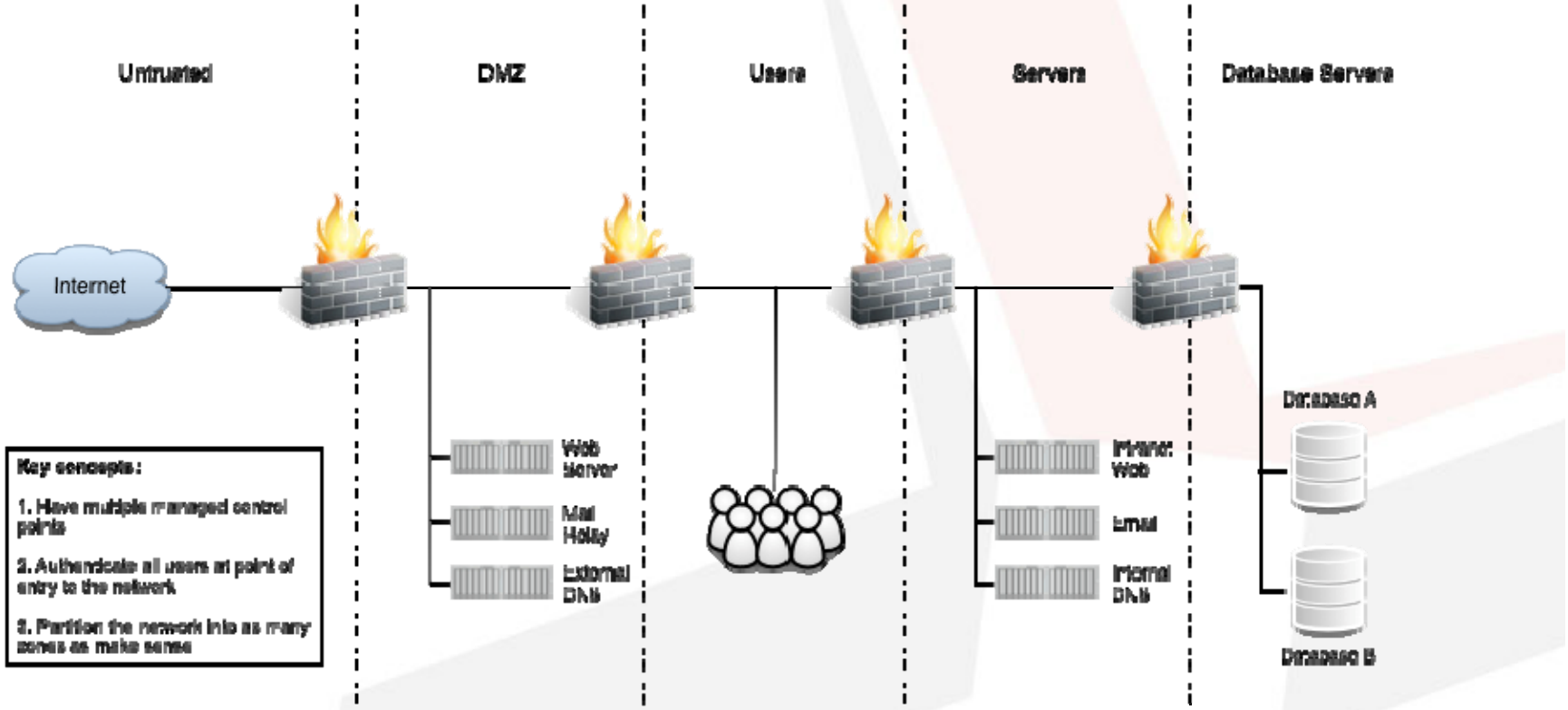


Source: Immunity Inc.

Common Pitfalls and Solutions

1. Network architecture

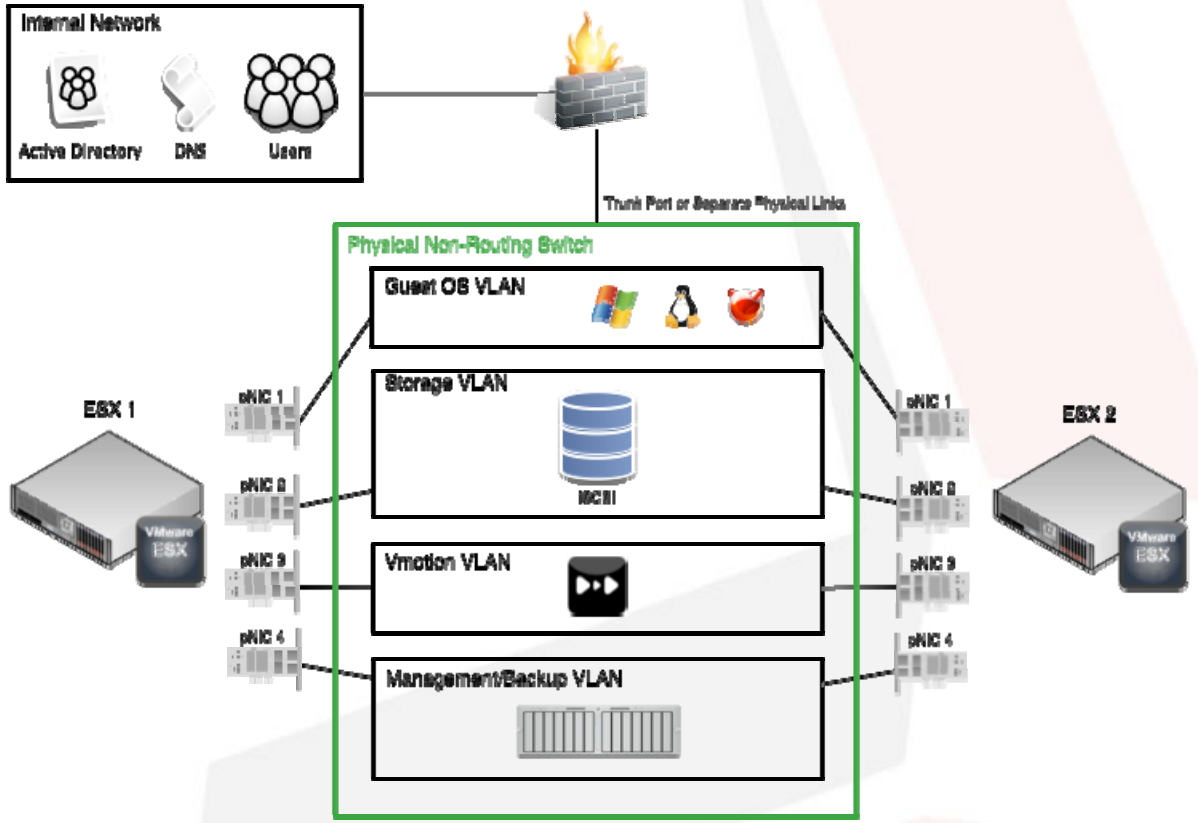
- Traditional (secure) network architecture



1. Network architecture cont.d

- Secure VM implementation

1. Isolate users from virtual machine networks
2. Isolate the infrastructure-related networks



Common Pitfalls and Solutions

Does anyone have any comments on the proposed design?

Other considerations:

- Blind Spots – traffic between VM's; vulnerabilities, malware, worms, etc
- No Access Control between VM's
- Live Migration - propagation of malware

Common Pitfalls and Solutions

2. Configuration Management

- Established best practice in traditional enterprise environments
- Can be more challenging in virtual environments
- Secure at deployment and maintain this position going forward
- Implement appropriate tools to enforce defined configuration standards
- Virtualisation introduces some new components that must be secured

2.1. Securing the Virtual Machines

- Secure virtual machines as you would secure physical machines
- Create a library of trusted virtualised server builds
- Use resource management to control server resources

2.2. Securing the Service Console (COS)

- Limit access based on business requirements
- Secure the root account
- Implement directory based authentication wherever possible
- Do not run additional software or services inside it
- Limit executing arbitrary commands and executables
- Apply patches
- Implement proper audit trails
- Do not use the service console unless necessary

2.3. Securing the Remote Command Line Interface

- Only necessary in ESXi
- Runs as a Debian Linux Guest appliance

OR

- Runs as an application on Windows
- Limit access based on business requirements

2.4. Securing VI Client including Web Access

- Connects to host via API
- Allows you to connect to the console of the VM interactively
- Copy and paste by default can move data between systems
- Use terminal services or SSH instead

2.5. Securing VirtualCenter

- Enterprise solution for managing VM implementations which is extendable with SDK
- Runs on user installed and secured Windows
- Implement RBAC

2.6. Securing vSwitches

- Do not use promiscuous mode on network interfaces (default setting)
- Protect against MAC address spoofing
  - MAC address changes (permitted by default) – should be denied
  - Forged transmissions (permitted by default) – should be denied

2.7. Securing Storage ?

- Each VM only sees virtual disks that have been presented to virtual SCSI adapters
- OS within the VM cannot change its own storage access or interrogate the storage

Common Pitfalls and Solutions

3. Applying Patches

- Challenging in virtual environments. e.g. offline virtual machines and templates
- Numerous components to patch

4. Defining Roles and Responsibilities

- Must learn where virtualisation technologies are being used, what they are being used for and who are responsible for their management
- Who will administer the virtual network?

Common Pitfalls and Solutions

5. Limiting Privileged Access

- Excess privileges make it possible for people to make uncontrolled changes to critical systems
- Must integrate information security into the access management procedures
- Reduce access wherever possible and ensure some form of effective access control exists
- Audit user access routinely and adjust access

Common Pitfalls and Solutions

6. Integrate with Existing Change Management Processes

- All changes after deployment should be authorised, scheduled, and substantiated by change management
- Activating and deactivating VMs should also go through change management

VMware Security Direction

- vShield Zones
  - Runs as a security virtual appliance
  - Enables you to monitor, log and block inter-VM traffic within an ESX host or between hosts in a cluster
- VMsafe
  - API enables development of virtualisation-aware security solutions in the form of a security virtual machine that can access, correlate and modify information based on memory and CPU, networking, process execution, or storage
- Cisco Nexus 1000
  - Alternative to VMware distributed switch with added functionality
  - Operates inside the VMware ESX Hypervisor
  - Brings policy based VM connectivity, mobile VM security and network policy

Conclusion

- Historically trends and advances in IT outpace security requirements. e.g. 802.11 wireless
- Most current implementations of virtualisation are insecure
- Virtualisation can be secured with the right know how
- Its much easier to bake in security from conception
- The only way to know if your implementation is secure is to have it audited by independent experts

Q&A

Questions?

Jason Edelstein

Sense of Security Pty Ltd

info@senseofsecurity.com.au

Tel: +61 2 9290 4444

Final presentation is available at:

http://www.senseofsecurity.com.au/presentations/Virtualisation-Security-AusCERT2009.pdf