Separating Fact from Fiction - ESXi Hypervisor Security

Mike Foley, VMware, Inc
Yuecel Karabulut, VMware, Inc
Disclaimer

• This presentation may contain product features that are currently under development.
• This overview of new technology represents no commitment from VMware to deliver these features in any generally available product.
• Features are subject to change, and must not be included in contracts, purchase orders, or sales agreements of any kind.
• Technical feasibility and market demand will affect final delivery.
• Pricing and packaging for any new technologies or features discussed or presented have not been determined.
We Would Like to Talk About Three Things Today

1. Virtualization Security: Fact vs. Fiction
2. Foundational Platform Security Solutions
3. Operational Security – Where the REAL Threat Is
Trusted by These Security Teams and 500k+ More
Security Concerns – Fact or Fiction
What Are You Most Concerned About?

“We are concerned about internal threats”
Example: Malicious privileged VI admin behavior in branch offices
What Are You Most Concerned About?

“We are concerned about VM escape scenarios”
Example: Guest-to-host-attack by exploiting a potential vulnerability in the VM process
What is the More Likely Scenario?

VM Escape
or
Operational Security Threats
What is the More Likely Scenario?

- **Probability**
- **Cost**

<table>
<thead>
<tr>
<th>Probability</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM Escape</td>
<td></td>
</tr>
<tr>
<td>Operational Security Threats</td>
<td></td>
</tr>
</tbody>
</table>
Fact vs. Fiction – VM Escape

**Fiction**
- VM Escape is considered a “Primary” threat by some security professionals

**Fact**
- There is a lot of *theoretical* intent to prove it!
- Known/past attempts took advantage of since patched vulnerabilities
  - In many cases were done NOT on VMware or with Type 2 hypervisors
- It’s very *hard* to do!
  - If it was easy you’d be reading about it on social media!
Why is VM Escape Really Hard to Do?

- Proven VM Isolation and Evolving Architecture
- Secure Software Development Lifecycle
- Minimum Attack Surface
- World Class Systems Security Engineers
Just the facts!
Layers of Isolation and Protection

Instruction Isolation
Memory Isolation
Device Isolation
Network Isolation
Noisy Neighbor Isolation
Storage Isolation
Memory Protection
Instruction Isolation

Virtual machines don’t have access to Physical Ring 0

Virtualized Privilege Levels

Hardware Privilege Level

VMM

Physical Ring 0

Physical Host

Virtual CPU

User Apps

Guest OS

OS Requests Trap to VMM without Binary Translation or Paravirtualization

Ring 3

Ring 2

Ring 1

Ring 0

Hypervisor

Instruction Isolation

Virtual machines don’t have access to Physical Ring 0

Virtualized Privilege Levels

Hardware Privilege Level

VMM

Physical Ring 0

Physical Host

Virtual CPU

User Apps

Guest OS

OS Requests Trap to VMM without Binary Translation or Paravirtualization

Ring 3

Ring 2

Ring 1

Ring 0

Hypervisor

Instruction Isolation

Virtual machines don’t have access to Physical Ring 0

Virtualized Privilege Levels

Hardware Privilege Level

VMM

Physical Ring 0

Physical Host

Virtual CPU

User Apps

Guest OS

OS Requests Trap to VMM without Binary Translation or Paravirtualization

Ring 3

Ring 2

Ring 1

Ring 0
Memory Isolation – VM to VM and VM to Host

Hypervisor managed guest memory page tables Isolated via CPU virtualization extensions (HWMMU)

Host and Virtual Machine Page Tables are completely inaccessible to each other
Device Isolation: Guests Only See What They Are Allocated

VM Kernel and VM Monitor mediate access to the physical resources, and all physical hardware access takes place through the VM Kernel.
Network Isolation at the vSwitch level

vSwitches are not routers!

To route packets between vSwitches you need something else.

Example: “Can a VM on vSwitch 1 see a VM on vSwitch 2?”
VLAN’s and vSwitches – No Hopping Allowed

- MAC Flooding? Not vulnerable
- 802.1q and ISL tagging? Not vulnerable
- Double-encapsulation Attacks? Not vulnerable
- Multicast brute-force Attacks? Not vulnerable
- Spanning Tree Attacks? Not vulnerable
- Random Frame Attacks? Not vulnerable
- VLAN Hopping? Native VLAN is not used
Operational Security – Where the REAL Threat Is
Fact vs. Fiction – Operational Security

Fiction
• Operational Security is considered a “Secondary” threat by security professionals

Fact
• Threat/Risk Management is not well understood
• Least Privilege is NOT widely adopted
  • Common ROOT passwords
  • All admins have vCenter privileges
  • Actions are not tied to policy
• Patching ESXi is not a priority
• Compromise the Admin, get access to the infrastructure
Least Privilege – RBAC Security Policy Enforcement
Least Privilege – Workflow-based Security Policy Enforcement

• Leverage VMware Orchestrator to limit privilege exposure
• Consider VMware vCAC for workflow approvals
• Example:
  – Remove “Delete VM” from Admin Role
  – Replace with vCO action
  – Use vCAC for approval workflow
Least Privilege – Workflow-based Security Policy Enforcement

• Leverage VMware Orchestrator to limit privilege exposure
• Consider VMware vCAC for workflow approvals
• Example:
  – Remove “Delete VM” from Admin Role
  – Replace with vCO action
  – Use vCAC for approval workflow
I Can’t Help You if you Don’t Patch!
You protect your physical datacenter with this guy...
...and this is how you protect your virtual datacenter?
Isolate Your Management Interfaces

Limit access to vCenter and ESXi with a dedicated Management Network
Takeaways

• VM Escape
  – VMware works hard to mitigate any and all potential threats in this area

• Real Threat Vectors
  – Continuous Threat Analysis
  – Operational Security
    • Adopt Least Privilege – RBAC and Workflow-based Security Policy Enforcement
    • Patch your systems!
    • Isolate your Management Interfaces
  – Network
    • Embrace Virtualized Networking and Micro-Segmentation (Go to the NSX sessions for more info!)
Questions?
Online Resources
ESXi Security Whitepaper and vSphere Hardening Guide

Whitepaper

Hardening Guide
VMware vSphere Beta

- Help shape the future of vSphere
- Gain visibility into features and technology that may be in upcoming versions of vSphere
- No nominations required. Open to everyone!
- [http://www.vmware.com/go/vspherebetaq2](http://www.vmware.com/go/vspherebetaq2)
Thank You
Fill out a survey

Every completed survey is entered into a drawing for a $25 VMware company store gift certificate
Separating Fact from Fiction - ESXi Hypervisor Security

Mike Foley, VMware, Inc
Yuecel Karabulut, VMware, Inc