The Virtualization Security Landscape: What's Changed?

Dave Shackleford
IANS
Virtualization Security: Then and Now

- We started this discussion in 2004-2005
- What’s changed?
  - First, we’ll cover threats to virtual environments and risks we face
  - Next, we’ll talk controls – both built-in and 3rd-party options
  - Architecture considerations for virtual environments make a difference too – anything new here?
- I’ll also cover some “lessons learned” and things I’ve observed along the way
Virtualization Threats and Risks
Threats to Virtualization

- Threats to virtualization infrastructure usually target vulnerabilities in various products
  - There have been numerous vulnerabilities in major virtualization products since 2008
- Some threats are more focused on hypervisor compromise
  - Hardware chipset virtualization
  - Architecture
  - Software
- Others are focused on management components, storage, etc.
Operational Risks

- **VM Sprawl**
  - Lack of change and configuration management controls
  - Poor inventory maintenance
- **Lack of visibility**
  - Inside the host system
  - VM-to-VM traffic across virtual switches
- **Separation of Duties**
  - Often, virtualization handed to an existing Windows admin team
- **Too many rights/privileges**
  - Both people AND VMs
  - Management components and services may have extensive privileges
Vulnerabilities

- VMSA-2009-0006
- Critical flaw in ESX 3.5, Workstation, etc.
- Code execution from VM Guest to Host
  - Overflow flaw in VM display driver

Immunity’s Kostya Kortchinksy wrote a tool called Cloudburst that exploited this flaw. In this screenshot, the Calc.exe program is run from the Guest on the Host.
Vulnerabilities: The Other Guys

- **Microsoft MS11-047:**
  - Critical DoS vulnerability in Hyper-V on Windows Server 2008
- **MS10-015:**
  - Elevation of privileges in Windows kernel
  - Affects Hyper-V systems running on Windows 2008
- **Citrix CTX123456:**
  - Authentication Bypass in XenServer 5 and 5.5
- **Citrix CTX129228:**
  - Credential Disclosure in XenServer 5.6
VM Detection and Fingerprinting

- VMs can be identified in a number of ways:
  - VMware VMs have a (default) MAC address starting with **00-05-69, 00-0c-29, 00-1c-14** or **00-05-56**
  - Registry entries include obvious strings like “VMware”, “esx”, and “vmx”
  - Communications bus with embedded “secret” such as “VMXh”
  - Memory locations of data structures like the Interrupt Descriptor Table (IDT)
- VM Detection can tell an attacker a lot: other VMs are close by, a host hypervisor is there, etc.
VM-aware Malware

- Building on VM detection – VM-aware malware has been around since 2006
  - Many Phatbot and Agobot variants have VM detection built in
- The Storm Worm leveraged VM detection techniques to put itself to sleep in VMware or Microsoft Virtual PC environments
  - Looks for the VMXh communications bus “password”:

```
00401146 . B8 68584D56     MOV EAX,564D5868
00401148 . BE 00000000     MOV EBX,0
00401150 . B9 0A000000     MOV ECX,0A
00401155 . BA 58560000     MOV EDX,5658
0040115A . ED              IN EAX,DX
0040115B . 81FB 68584D5F   CMP EBX,564D5868
00401161 . 0F9445 E7      SETE BYTE PTR SS:[EBP-19]
00401165 . 5B              POP EBX
```
VM Escape & Virt Rootkits

- VM Escape: Attackers “break out” of a running VM to hijack the hypervisor platform
- Plenty of “near miss” directory traversal flaws:
- Joanna Rutkowska created a POC thin VMM that encapsulates the underlying host OS
  - Blue Pill in AMD (2006)
  - Intel vPro TXT (2009)
More Valid Threats and Attack Scenarios

- Data Interception and MITM Attacks
  - Memory migration with vMotion is in cleartext
  - An attacker on the VMkernel network could sniff the contents of memory easily
- Backdoor shells and shell connectivity
  - Limited version of Netcat is built-in to modern ESXi
- VMware Communications Channel is still available, although limited
- VASTO Toolkit for Metasploit
  - Guest Stealer, VI Lurker
2012: What’s Real vs. Hypothetical?

- VM Escape has not proven to be a significant threat in the “real world”
- Hypervisor attacks are real, though – it could definitely happen, and we know this
- Most malware actually doesn’t evaluate for VMs anymore – virtualization is too ubiquitous!
  - Code is still there, though
- Biggest challenges are operational
  - Patching, configuration, managing inventory/sprawl
What should security teams focus on?

- Do not buy into vendor FUD!
  - Most virtualization threats are operational
- Focus on:
  - Proper hardening
  - PATCHING (!!!)
  - Change control
  - Monitoring
  - Privilege control and separation of duties
- Keep up with new vulnerabilities and research for your virtualization platforms though!
Virtualization Security Controls and Tools
VMware vSphere

- Numerous security controls built in
  - Limited virtual switch security policies
  - Basic hypervisor controls for access control (limited TCP Wrappers), remote access (SSH), user/groups, etc.
  - ESX/ESXi firewall, stateless and very simple
  - ESXi has Lockdown Mode that can be enabled, restricting hypervisor management
  - Syslog support with log rotation
  - ESXi package integrity levels

- VMware Hardening Guidance is up to date and regularly maintained
  - Extensive guidance for different security levels
  - Current version is 4.1
Microsoft Hyper-V

- Hyper-V Hypervisor Security Model
  - Host OS and Hypervisor run in separate address spaces
  - All Guest VM device traffic bypasses hypervisor
  - No shared memory for Guests

- Few controls built-in:
  - Only VLANs for virtual switches
  - AzMan for user/group/role control and access

- Windows Server 2008 controls can be used:
  - Anti-malware, encryption like BitLocker, etc.

- Hyper-V Security Guide is out of date (2009)
  - Minimal guidance on Windows 2008 hardening and AzMan
Citrix XenServer

- Many Linux hardening and security steps will be applicable for Xen:
  - Set File Permissions on Domain files
  - Control root/user access and passwords
  - Control remote access (VNC, SSH)
- VLANS can be configured for the virtual network
  - Promiscuous mode can be enabled
- SSL and SSH can be configured with certificates/keys
- IPTables-based firewall is in place
- SELinux is installed by default and available
- **Passwords are not shadowed.**
- XenServer Security Guidance is almost non-existent
  - Some guidance from CIS on v3.2 (ancient)
## Platforms: A Quick Summary

<table>
<thead>
<tr>
<th>Feature</th>
<th>vSphere</th>
<th>Hyper-V</th>
<th>XenServer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stateful Firewall</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Role-based access</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Thin Footprint</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Syslog support</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>vSwitch Monitoring</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Built-in vSwitch Security Policies</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSH/SSL support</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Detailed Hardening Guidance</td>
<td>✔️</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Virtual Switches

- Cisco Nexus 1000v offers enterprise capabilities:
  - SPAN ports
  - VM-aware policies
  - vPath traffic shaping/monitoring
- The Open vSwitch project has a number of the same features as Nexus
  - Flow
  - SPAN
  - QoS
Virtual Firewalls and IDS/IPS

- Virtual firewalls can augment, but usually don’t replace, existing firewall architecture and strategy
  - Can your physical firewall handle VM↔VM traffic?
  - Can your physical firewall accommodate specialized traffic like vMotion?
- Another top concern with virtualization is monitoring traffic inside the virtual network
  - Virtual networks have been viewed as a “black box”
  - Determine whether you will use commercial or open-source tools
Virtual Firewall Product Examples

- VMware vShield Edge and vShield App
- Juniper vGW Line
  - Formerly Altor virtual firewall
  - Includes firewall, IDS, and antivirus capabilities
- Reflex Systems vTrust
  - Network policy enforcement, quarantine, and segmentation
- Catbird VMShield
  - VM activity monitoring, packet filtering and deep inspection
  - VM quarantine, NAC, VM policy & configuration audit
IDS/IPS Product Examples

- **Sourcefire**
  - These are interoperable with their physical counterparts
  - Can also integrate with VMware vShield products

- **HP TippingPoint**
  - Option 1: Virtual “tap” sends traffic to a physical IPS
  - Option 2: Virtual IPS and virtual tap
  - Management console takes VM policies and lifecycle into account

- **McAfee Network Security Platform**
  - Not a virtual IPS!
  - Uses an agent to send traffic to a physical IPS
  - Also provides VM quarantine and integration with ePO host-based IDS/IPS
New Anti-Malware and HIDS Options

- These have evolved more slowly
- Considerations include:
  - Resource Consumption
  - Integration capabilities
  - Architecture
- vShield Endpoint
  - VMware partner-driven anti-malware
- OSSEC
  - Freely available HIDS and log monitoring agent
  - Can be used with VMs and management servers
Virtual Encryption

- As virtual machines are comprised of sets of files, encryption processes and tools may need to change as well to accommodate how virtualization works.
- Data can be encrypted in several ways:
  - File/folder encryption
  - Full disk encryption for VMs
  - Full VM encryption
  - Specialized encryption (DB, Email)
What’s Important for You?

- On new vendor offerings:
  - To inspect VM-to-VM traffic, you’ll need deeper integration with the virtual platforms
  - “Fast path” integration can offer performance improvements
  - **Use what you have first! Then add virtual solutions.**
- Virtual firewalls are fairly mature today
- Virtual IDS/IPS are getting there
  - Virtual appliances are most common
- Virtualization encryption is an area to watch, especially for cloud implementations
Virtualization Security Architecture Options Today
Virtualization Security Architecture

- Security operations may need to be architected differently to function properly or optimally within virtual environments
- This applies for network, host, and really any security tools and operations
- Many new architectures are being developed for network access controls and traffic monitoring
- The use of VDI and private clouds can have definitive security impacts, both good and bad
Virtual Firewall Architecture

- Virtual firewalls are used to define trust zones inside a virtual platform.
- These can be created for every virtual switch.
  - Or be bridged across multiple switches.
IDS/IPS Options: SPAN ports

- **Option 1: Span all traffic from physical switch**
  - No virtual IDS
  - SPAN pNIC traffic to a monitoring port on the switch
  - Multiple VM traffic can be significant for one NIC, thus flooding a switch backplane

- **Option 2: Set up a Nexus or Open vSwitch**
  - Port this traffic to a virtual IDS or a pNIC that connects to a physical IDS
  - This is a mature option that most enterprises find attractive
More IDS/IPS Architecture Options

Dedicated IDS VM with separate vNIC for monitoring

The VM must run some sort of bridging or routing to pass packets through one NIC to another
A New Idea: VDI for Security?

- Desktop environments can be very tightly controlled by administrators
  - Individual users are less able to install software and make other unauthorized changes
- Configuration management and patching is more easily centrally controlled
  - Virtual machines can be easily cloned and generated via “gold build” templates
- User data is stored centrally and desktop environments are ephemeral
  - Improved backup/restore, DR/BCP for users
Network Architecture Changes

- More organizations are building private cloud infrastructure on top of virtualization
- Networks supporting private clouds will need several major architecture changes/considerations
  - Defining and limiting access at the “edge”
  - External vs. internal connectivity
  - Network isolation and segregation
  - Management networks
Virtual Network Design Models

- VMware outlines 3 models:
  - Partially collapsed DMZ, separate physical trust zones
  - Partially collapsed DMZ, virtually separate trust zones
  - Fully collapsed DMZ

- These differ in terms of where and how segmentation and isolation take place
  - A fully collapsed architecture is becoming more of a reality
A Fully Collapsed Virtual Network

Internetz.

Circuit.

Your Whole Network!
OK, Just Kidding.
A Fully Collapsed Virtual Network (for REAL)

Guidance for Security Pros

- Implement virtual firewalls for improved access control between VMs and VM segments
- Be wary of fully-collapsed architectures
  - A partially collapsed model is likely best for many organizations today
- Leverage physical IDS/IPS where possible
  - SPAN from vSphere or Nexus 1000v/Open vSwitch
- Host-based tools must take resource consumption into account
  - Many can still be resource hogs, test carefully!
Wrapping Up: What’s to Come
Virtualization Today and Tomorrow

- Virtualization technology is only growing in maturity and adoption
- Security, for better or worse, is along for the ride
- A key point: Do *not* think security will drive innovation in the virtualization space!
  - If it does, it’s likely a byproduct!
- This doesn’t mean virtualization and security can’t get along
  - Just remember that virtualization is all about speed and operational efficiency – not security
So...Where are we headed?

- Security has a few key areas of evolution ahead with regard to virtualization (and cloud)
  - Architecture and design: Network design, use of virtualization for innovative security architecture
  - Security product adaptation: As we covered already, we’ll need to adapt existing tools and develop new ones to work in these environments
  - Improved hypervisors and virtualization platforms: Thinner, simpler hypervisors with more security

- Let’s cover each in a nutshell with examples
Examples of Virtualization Security Evolution

- **Architecture**: New designs that allow for improved segmentation and control
  - Example: VDI for remote access
  - Example: Virtual DMZs

- **Product Adaptation**: Security tools that are changing to work in virtual environments
  - Example: HyTrust Virtual Policy control
  - Example: High Cloud Security Full VM Encryption

- **Hypervisor Improvement**: Less footprint, more security
  - Example: ESXi Direct Console with ESXi v5 firewall
  - Example: ESXi embedded
How to Apply What We’ve Covered

- In the next 3-6 months, you should consider the following:
  - Add patch and vulnerability assessment for any virtual platforms you maintain
  - Ensure threat models and risk management processes incorporate virtualization scenarios
  - Do not succumb to FUD! Virtualization security is definitely achievable, almost entirely in operations
  - Evaluate new virtual security tools to augment or even replace existing tools like firewalls and IDS/IPS
  - Consider architecture changes and adaptations including VDI and more fully collapsed infrastructure
Conclusion and Wrap-Up

Thanks for attending!
Questions?

Contact info:
dshackleford@iansresearch.com