NEbraskaCERT

NEbraskaCERT's Cyber Security Forum

Virtualization Security Update

September 21, 2011

Michael Hoesing CISSP, CISA, CCP, CIA,
CFSA, CMA, CPA, ACDA

mhoesing@mail.unomaha.edu

402 981-7747

University of Nebraska Omaha

a CAE IAE institution

Super legal mumbo: I’m broke, don’t sue me.

Virtualization Security Update – Agenda

- Intro, Background, Scope
- vShpere 5 released July 2011 - things have changed
- PCI Security Council June 2011 - a whitepaper with guidance (kinda, finally)
- VMware Hardening Guide for 4.1 April 2011 - should be a basis for your build policy/standard/procedure
- ISACA Virtualization Audit Program Feb 2011 - what "those people" want now
- NIST SP 800-125 Jan 2011 - me too document
- Center for Internet Security vShpere 4.1 Benchmark Dec 2010 - with an XCCDF testing script
- Other - VMworld Aug 2011 - sorry no funding no attendance

A.) Intro, Background, Scope

Intro, Background, Scope

- Important – who has not virtualized at least some of their server population?
- Scope – servers (storage, and other things can be virtualized, we will focus on servers this hour)
- Scope – VMware products, they have the majority of the market (HyperV, Citrix, KVM,…. At lot of others out there, wish I had more time and a funded lab)

RISKS & CONTROLS – a list of 10

1. **VM/Guest Sprawl**
2. **Host Mis-Configuration**
3. Network Segmentation
4. Remote Access

- Policies, Procedures, Inventory Practices, Reporting, Assessment
- Standards, Monitoring, Assessment
- Deploy Segregated Management, Production and IP Storage Networks
- SSH , SSL, access & account controls

RISKS & CONTROLS – a list of 10 (cont)

5. User Account Access & Roles
6. Single Point of Failure
7. Integration
8. Staff Skills
9. Architecture (Blue Pill)
10. Software Licensing
11. I lied # 11 Appliances
12. #12 Guest Escape VMSA-2009-0006

- Policies, Procedures, Least Privilege
- Backups, Continuity Planning
- Strategic Architecture, Capacity Planning
- Training
- Physical Security
- Policy, Monitoring
- QA, Certification Processes, Vendor Mgmt
- Patch Process

B.) vSphere 5 – July 2011

vSphere 5

- Released July 2011
- Memory based pricing is new, and not popular (VMware raised to ceiling later 2 processors, 192 GB)
- ESX COS is gone, ESXi the only choice
- ESXi has hypervisor and console all on the same partition, faster (vendor says)
- ESXi 5 has a firewall (iptables) ESXi v1-4 did not
- No (if configured as suggested) console access, all access is remote using vendor tools
- Use vMA, remote CLI, and PowerCLI for audit metric gathering or vCenter

vSphere 5 - 2

- TPM (Trusted Processing Module) recognition available (Intel's TXT or AMD's SEM , soon)
- AD authentication carried forward from ESXi 4.1
- Hope they Fixed These in 5 (ESXi 4.1 issues)
  - ➢ Logs removed upon reboot ☹ root password not set during installation
  - ➢ Tech Support Mode (from console)
  - ➢ Remote Tech Support Mode (SSH), accesses **Single User Mode** (root without any password if not set at default, even with password root SSH is enabled)
  - ➢ Reset System Configuration **– resets an empty root password** (watch iLO and iDRAC)
- Evaluation https://www.vmware.com/tryvmware/?p=vmware-vsphere5-ent&lp=default&rls=com.microsoft:en-us:IE-Address&ie=UTF-8&oe=UTF-8&sourceid=ie7&rlz=1I7ADRA_en

C.) PCI Security Council June 2011 - a whitepaper

PCI Security Council

- https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf
- Promised since 2009
- In Scope – one guest, then the host is in, and all guests on that host
- Watch the narrative vs the Requirements and Security Assessment Procedure text (5.1 AV “must” in the RSAP, “may be” in the Virtualization Considerations)
- Intro confuses the definitions of Hypervisor and VM
- Cloud IaaS, customer should control vendor’s hypervisor?

D.) VMware Hardening Guide for 4.1
April 2011

VMware Hardening Guide 4.1

- http://www.vmware.com/files/pdf/techpaper/VMW-TWP-vSPHR-SECRTY-HRDNG-USLET-101-WEB-1.pdf
- Covers VMs and the vCenter, in addition to the hypervisor and COS
- Shows how the protect against single user mode boot
- Differentiates techniques for ESX and ESXi
- Differentiates Risk Levels – Enterprise, DMZ, Specialized
- Use as a base, embellish with CIS & DISA

VMware Hardening Guide 4.1 -2

- Covers VMsafe connections
- ESXi lockdown mode with DCUI disabled, no console access, must only use vendor management tools (sysadmins going to like that?)
- Nice job with remote access tools
- Lockdown mode disables console except for local (DCUI), watch iLO and iDRAC
- Host Profiles, for assessment and remediation
- Update Manager guidance
- Specifically mentions Tripwire for FIM

E.) ISACA Virtualization Audit Program Feb 2011

ISACA Virtualization Audit Program

- Started with a whitepaper Oct 2010 http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Virtualization-Benefits-and-Challenges.aspx
- Then the audit program in Feb 2011 http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/VMware-Server-Virtualization-Audit-Assurance-Program.aspx (must be an ISACA member for these two documents)
- GRCish, ERMish, high level, process emphasis
- Lots about maturity models

ISACA Virtualization Audit Program - 2

- 3.4 VMware Server, anyone using that for enterprise virtualization ??
- 4.1.1.1 Use Hardening Guides (does not mention CIS, despite CIS being a sponsor)
- 4.1.2.1 “Select Configure Root Password” where is that in ESX? (it is on the DCUI for ESXi)
- 4.1.3 “ESX Lockdown” , lockdown is only available on ESXi
- 4.1.6.1 requires patching using Update Manager, while that is the best way, it is not the only way

ISACA Virtualization Audit Program - 3

- 4.1.9.1 assessment tools, Bastille –does not have a VMware module use Bastille only in assessment mode, DISA STIG is a hardening guide not an assessment tool, DIS does have a hardening tool (security readiness review, careful not to apply changes automatically), forgot to mention the CIS XCCDF assessment script
- 4.2.1.5 disable SSH (how do you configure syslog?)
- 4.5 capacity planning covered, that is good given how easy it is to have sprawl
- Appendix B – nice detail, audit performance?

F.) NIST 800 – 125 January 2011

NIST 800-125

- http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf
- Mentions positive and negative aspects (snapshots)
- Nice discussion of decommissioning, planning topics not generally in the other documents
- Nice introduction without the detail
- Makes a good first read

G.) Center for Internet Security vShpere 4.1 Benchmark Dec 2010 - with an XCCDF testing script

CIS ESX 4.1 Benchmark

- CIS Benchmark (free) http://benchmarks.cisecurity.org/en-us/?route=downloads.show.single.esx4.100 (note: I am not independent in regards to this damn fine benchmark document.)
- CIS Computer Assessment Tool (CIS-CAT) membership required http://benchmarks.cisecurity.org/en-us/?route=downloads&original=downloads.audittools (note: I am not independent in regards to this damn fine ESX XCCDF assessment script.)
- Focus on the hyperviser and the COS
- VM configuration covered as they interact with the host
- Multiple professional inputs, vendor and non-vendor

CIS ESX 4.1 Benchmark - 2

- CIS vs VMware hardening
  - ➢ CIS a few more hardening techniques (services, iLO iDRAC, banners)
  - ➢ VMware covers vCenter, and VMs more
- CIS CAT XCCDF
  - ➢ Some test steps gather the metric, hold that answer to the standard, then grade as pass/fail (password metrics)
  - ➢ Some test steps display the metric(s) for the assessor to evaluate off-line (partitions)

H.) Other

Other

- VMworld 2011 – sorry didn’t go, but I hear a lot of discussion over pricing, vSphere 5 allows better storage control (movement & management)
- DISA STIG (not updated since 2008) http://iase.disa.mil/stigs/os/virtualization/esx.html