Virtualization Security & Audit

John Tannahill, CA, CISM, CGEIT, CRISC
jtannahi@rogers.com
Session Overview

- Virtualization Concepts
- Virtualization Technologies
- Key Risk & Control Areas
- Audit Programs / Checklists
Virtualization Concepts

- **Type 1:** Bare Metal Hypervisor
  - Host – ESXi Server
  - Hardware

- **Type 2:** OS-Based Hypervisor
  - Guest OS
  - Guest OS
  - Hypervisor
  - Host OS e.g. Linux
  - Hardware
Virtualization in the Organization

• Key audit scoping issue is understanding of use of virtualization in the organization

• Server Virtualization e.g. x86 hardware (session focus)

• Storage Virtualization

• Network Virtualization

• Desktop Virtualization (VDI)
Virtualization Technologies

• VMware vSphere
• Microsoft Hyper-V
• Azure Hypervisor
• Oracle VM
• Linux KVM
vSphere

VMware vCenter Server

Manage

VMware vSphere (3 instances)

Source – VMware
Oracle VM

- X86 server virtualization
- Xen hypervisor technology
- Supports Windows, Linux, and Oracle Solaris guests
- Oracle VM components
  - Oracle VM Manager: web based management console to manage Oracle VM Servers.
  - Oracle VM Server: includes a version of Xen hypervisor technology
  - Oracle VM Agent to communicate with Oracle VM Manager for management of virtual machines
  - Minimized Linux kernel as Dom0
VMware Horizon View
(source – Wikipedia)

• VMware View provides remote-desktop capabilities to users. A client desktop operating-system – e.g. Windows 7 runs within a virtual environment on a server.

• VMware View components:
  – VMware vSphere for Desktops (includes ESXi)
  – VMware vCenter Server
  – View Composer (advanced View management, with automation and cloning)
  – View Manager (administration of the View Environment)
  – View Client (communication between View and the desktop OS)
  – VMware ThinApp (application virtualization)
  – View Persona Management (user profile management)
  – vShield Endpoint (offloaded desktop antivirus)
Best Practices for Mitigating Risks in Virtualized Environments

(source – cloudsecurityalliance.org)

• VM Sprawl
• Sensitive Data Within a VM
• Security of Offline and Dormant VMs
• Security of Pre-Configured (Golden Image) VM / Active VMs
• Lack of Visibility Into and Controls Over Virtual Networks
• Resource Exhaustion
• Hypervisor Security
• Unauthorized Access to Hypervisor
• Account or Service Hijacking Through the Self-Service Portal
• Workload of Different Trust Levels Located on the Same Server
• Risk Due to Cloud Service Provider API
Defcon 20 - VASTO

ERPScan
Security Scanner for SAP

Invest in security
to secure investments

How to hack VMware vCenter server in 60 seconds

Alexander Minozhenko
Metasploit Framework

• Examples:
  – auxiliary/scanner/vmware/vmware_enum_users
  – auxiliary/scanner/vmware/vmauthd_login
  – auxiliary/scanner/vmware/vmware_http_login
  – auxiliary(poweron_vm)
Compromise-as-a-Service

Our PleAZURE

Felix Wilhelm & Matthias Luft
{fwilhelm, mluft}@ernw.de
Critical Security Controls - V6

• CSC 1: Inventory of Authorized and Unauthorized Devices
• CSC 2: Inventory of Authorized and Unauthorized Software
• CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
• CSC 4: Continuous Vulnerability Assessment and Remediation
• CSC 5: Controlled Use of Administrative Privileges
• CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
• CSC 7: Email and Web Browser Protections
• CSC 8: Malware Defenses
• CSC 9: Limitation and Control of Network Ports, Protocols, and Services
• CSC 10: Data Recovery Capability
Critical Security Controls – V.6

- CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- CSC 12: Boundary Defense
- CSC 13: Data Protection
- CSC 14: Controlled Access Based on the Need to Know
- CSC 15: Wireless Access Control
- CSC 16: Account Monitoring and Control
- CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps
- CSC 18: Application Software Security
- CSC 19: Incident Response and Management
- CSC 20: Penetration Tests and Red Team Exercises
Key Security Processes

• Configuration and Asset Management
• Security Architecture
• Secure Build Process
• Hardening Process
• Security Bulletin Monitoring Process
• Patch Management Process
• Privilege Management
• Vulnerability Management Process
NIST SP800-125 - Guide to Security for Full Virtualization Technologies

• Virtualization Security Overview
  – Guest OS Isolation
  – Guest OS Monitoring
  – Image and Snapshot Management

• Security Recommendations for Virtualization Components
  – Hypervisor Security
  – Guest OS Security
  – Virtualized Infrastructure Security
  – Desktop Virtualization Security

• Secure Virtualization Planning and Deployment
NIST 800-125-A Draft: Security Recommendations for Hypervisor Deployment

• Threats Areas:
  – HY-BF1 - Execution Isolation for Virtual Machines
  – HY-BF2 Devices Emulation & Access Control – such as Network and Storage (block) devices
  – HY-BF3 Execution of Privileged Operations for Guest VMs by the Hypervisor
  – HY-BF4 Management of VMs
  – HY-BF5 Administration of Hypervisor Host & Hypervisor Software

• Recommendations for hypervisor security baseline functions (vendor-neutral)
NIST SP800-125B
Secure Virtual Network Configuration for Virtual Machine (VM) Protection

• Network Segmentation Configurations for VM Protection
• Network Path Redundancy Configurations for VM Protection
• VM Protection through Traffic Control Using Firewalls
• VM Traffic Monitoring
vSphere 5.5 / 6

• Security Guide
• Hardening Guide
VM Hardening Steps

• Secure Configuration (Hardening)
• Security Patch Management
• Example Standards:
  – STIG
    • http://iase.disa.mil/stigs/stig/index.html
  – CIS Benchmark
    • http://cisecurity.org
  – VMware Best Practice Guides
ESXi Server 5.5 – Coverage

CIS VMware ESXi 5.5 Benchmark

v1.0.0 - 08-04-2014

1 Install
2 Communication
3 Logging
4 Access
5 Console
6 Storage
7 vNetwork
8 Virtual Machines
   8.1 Communication
   8.2 Devices
   8.3 Guest
   8.4 Monitor
   8.5 Resources
   8.6 Storage
   8.7 Tools

**Rule Title:** The VMM must limit the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number of sessions.

#### Discussion
Enabling lockdown mode disables direct access to an ESXi host requiring the host be managed remotely from vCenter Server. This is done to ensure the roles and access controls implemented in vCenter are always enforced and users cannot bypass them by logging into a host directly. By forcing all interaction to occur through vCenter.

#### Check Content
From the vSphere Web Client select the ESXi Host and go to Manage >> Settings >> System >> Security Profile. Scroll down to "Lockdown Mode" and verify it is set to Enabled (Normal or Strict).

#### or

From the vSphere Web Client select the ESXi Host and go to Manage >> Settings >> System >> Security Profile. Click edit on "Lockdown Mode" and set to Enabled (Normal or Strict).

#### or

**CCI:**

The information system limits the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number of sessions.

**NIST SP 800-53 Rev. 4** - A12.1
VMware Best Practice Guides

- VMware vSphere Hardening Guide
  - Virtual Machines
  - ESXi Hosts
  - Virtual Network
  - vCenter Server
  - vCenter Components
Storage Security

- NAS
- SAN
- Protocols
  - NFS
  - CIFS / SMB
Network and Firewall Security

• Minimize TCP/IP Services
  – Host and Guest VM’s
• Firewall and VLAN security
• Vswitch configuration
• Distributed Switches
Vmotion / Cloud Bursting

Source – VMware
Cloud Security Benchmarks

CIS Amazon Linux 2014.09 Benchmark
v1.0.0 - 01-06-2015
Other Audit Areas to Consider

- Software Defined Data Centre (SDDC)
- Micro segmentation
- Software Defined Networking (SDN)
- Hyper-convergence
- Containers
CIS – Docker Benchmark

CIS Docker 1.6 Benchmark
v1.0.0 - 04-22-2015
ISACA VMWare Audit Program

- Planning and Scoping the Audit
- Governance of the virtualized environment
- Pre Fieldwork Preparation
- VMware virtualized environment
- Compliance

- Control & Audit Objectives
Session Summary

• Use of Virtualization technology within Organization
• Understand key risks
• Understand technology and key controls
  – vCenter Security (Management)
  – ESXi Security (Hypervisors)
  – VM Security (Guest VM)
• Service and Cloud Provider Environments