HM hackmiami

Security Challenges in Virtualization Technologies

By @rodsoto

Disclaimer

- The following is a high level presentation about attack vectors and mitigation techniques of commonly used virtualization technologies (HyperV, Vmware, Citrix).
- This presentation is not extensive but aims at providing audience with basic knowledge and resources to continue further research.

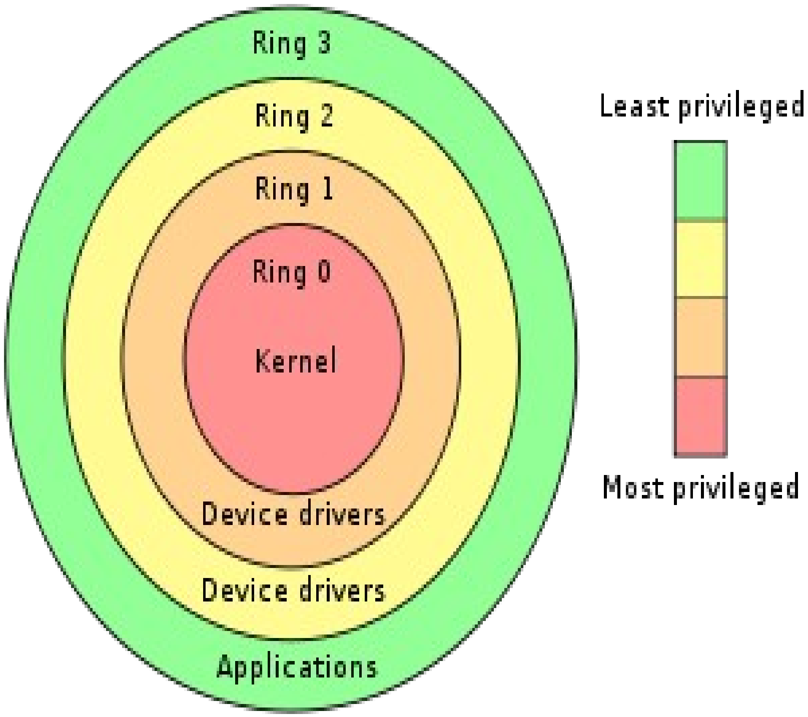
What are virtualization technologies?

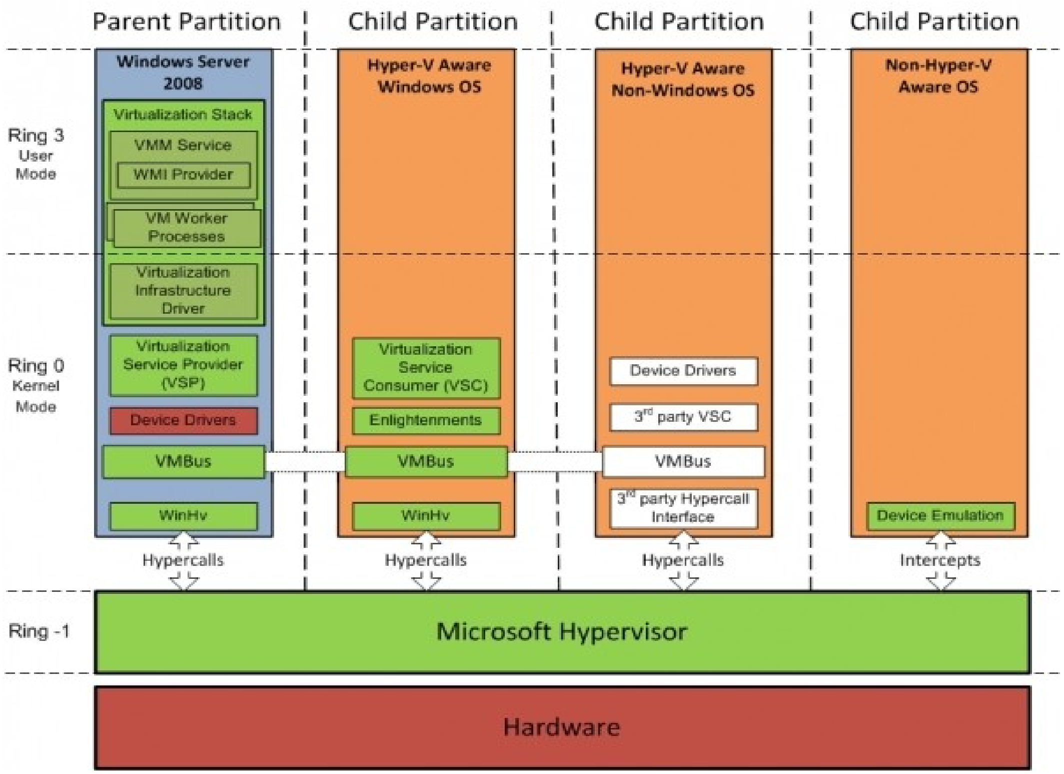
- Technologies that facilitate the creation of a technical artifact, such as a hardware platform, operating system (OS), storage device, or network resources.
- Types of virtualization are mainly hardware and software
- It all starts at the hypervisor which is the software layer that will run the virtual hardware, OS, storage device or network resources. There are two types of hypervisors:
  - Bare Metal: Installed directly on hardware (Example: Esxi, XenServer, Hyper-V 2008 R2)
  - Software Based: Run on top of OS on top of hardware (Example: MS Virtual Server, VirtualPC, Parallels, Vmwarefusion,etc).

Common uses of Virtualization Technologies

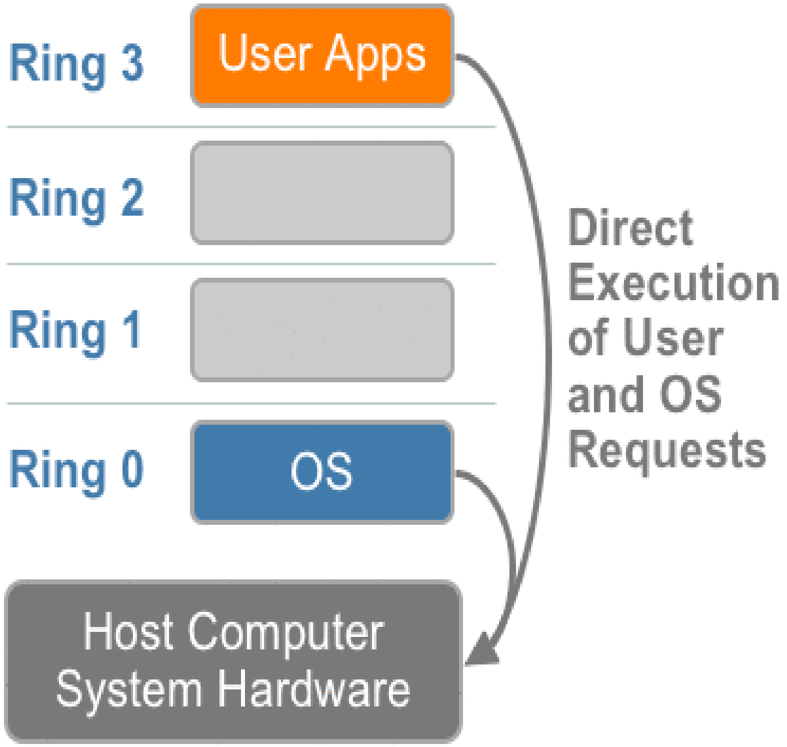
- Reduction of hardware/rackspace footprint (more servers in less space).
- Improve ratio between hardware/resource use (Memory, Storage, Networking, load balancing).
- Centralize management of resources, escalability, high availability, storage, memory.
- Ability to run Legacy applications on current hardware platforms. (Applications presented to clients that are not able to run them otherwise, Windows NT, or that app your org purchased and vendor went out of business).
- Is estimated than more than 16 percent workloads are already running on VM. With an expected growth of 50% in the next years.
-

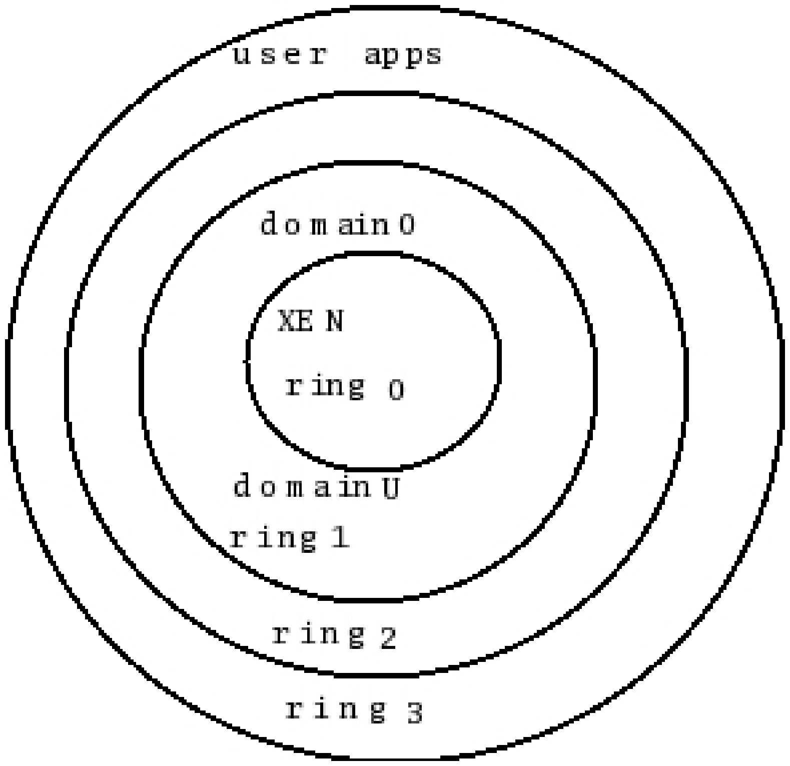
Hypervisors & x86 Privilege Rings





CPU Virtualization risks


Ring 3
User Apps
Ring 2
Ring 1
Ring 0
OS
Direct Execution of User and OS Requests
Host Computer System Hardware



CPUs from Intel and AMD offer x86 virtualization instructions for a hypervisor to control Ring 0 hardware access.

Security Challenges

- Virtualization technologies are here to stay. As they continue to replace physical systems and spread around organizations, there are certain virtualization related security challenges that come with the implementation of these technologies.
- These challenges are in addition to the common security items that most sys admins must face in an organization.

Security Challenges/ Attack Vectors

- The following are in general the most common attack Vectors related to Virtualization technologies.
  - Attack against web management interface (I.E Path traversal - CVE-2011-0426 CVE-2011-1788 CVE-2011-1789)
  - Attack services with direct link and privileges to Hypervisor. (Vcenter server runs on windows :) there is an Suse version too.)(Hyper-Jacking)
  - Attack management/administrative system (Escalate privileges through user impersonation)
  - Break in through vulnerable VM then escalate or escape hypervisor. (**CVE-2009-1244,CVE-2011-1751, CVE-2012-0217,**CVE-2012-3288)(VM-ESCAPE)
  - VLAN attacks. (ARP, Multicast BF, MAC Flooding, VTP attack), (I.E CVE-2005-4440)
  - Compromise of VM File (VM Theft)
  - Attack the Hypervisor itself (SSH, DDOS, SMB, Physical, etc)(CVE-2012-3289)
  - Exhaust Hypervisor resources (Over committing)
  - Attack Hypervisor management VM if present in the same VM network(I.E Vcenter_Server, XenApp)(VM Hopping)

Other challenges not limited to Virtualization but important in these environments

- Trust relationships
- Isolation and network management
- Configuration/Patch management
- Co-tenancy if in cloud environments
- Storage Guest to Guest, Guest to Host relationships
- Provisioning and resource management
- Separation of duties, PoLP in administration duties and users

Mitigation techniques

- Control physical access. Enable boot loader, bios passwds, DEP (Hyper-V). Same goes for remote access (iLO, DRAC)
- Check integrity of hypervisor packages prior to install, keep version log. (I.E Vmware TXT)
- Disable root login via SSH
- Not related just to Virtualization but disabling Administrator 500 on win machines is NOT a good idea you never know when you have to demote, unjoin or even go physical again. Ensure passwords are complex and most importantly remember them :).
- Isolate (Physically) management nic, never mix with production. (XenServer, Esxi webpages).
- Disable non necessary services, enable firewall.
- NEVER let your guests access datastores or share storage with Host.
- Try to have a physical V-Center, then create container as backup ISOLATED from VM Network. If you decide to go all the way virtual with main services such as DNS, AD, LDAP, EMAIL you should have a PHYSICAL back up.
- ISOLATE management, storage, test/dev, production networks.
- Enforce PoLP, SoD in Virtual Management administrators. Create and isolate administrative groups with credentials and privileges that will limit exposure in case of breach.
- Even if Isolated or segmented ENCRYPT if possible all communications between Hypervisor, Management consoles, Storage, network devices.
- Segment and enforce access to storage volumes.

Mitigation Techniques II

- Prevent over committing of resources. Manage resource assignments by segment and importance in infrastructure (I.E Virtual Machine Attributes, Resource Pools, FT, HA, DRS, Load Evaluators, MS SSCM)
- Security measures on the guests should be applied as well as they were physical (Antivirus, Firewall, Logs, patch management, Vcenter Protect, WSUS, SELinux, etc).
- Change control management, configuration management, PREVENT VM SPRAWL (I.E Vmware templates, Vmware Vcenter compliance checkers, Hyper-V Attack Surface reference workbook, etc)
- Apply Layer 2 attack countermeasures (I.E Prevent virtual Nics from going on promiscuous mode).
- Keep, index, prioritize, protect system, security, application logs in a centralized manner implement protections and failbacks (Use service accounts with limited privileges to write ONLY the logs, locate logs in secure location, prevent single point of failure).
- Do not import Virtual Machines from untrusted sources.
- Use TFA when possible.
- If in the Cloud AVOID Co-tenancy if possible.
- Goes without saying AUDIT, Pentest your infrastructure.

Further reading/research

- ISACA Virtualization Security Checklist http://mcaf.ee/ycz0u
- Support of Vmware TXT http://mcaf.ee/7av5u
- X-Force White Paper on Virtualization Security http://mcaf.ee/140wo
- Securing the Virtual Environment. Ottenheimer, Wallace

  http://www.amazon.com/dp/1118155483/ref=cm_sw_r_tw_dp_KhG0pb1YRN07D
- VMware Cloud Burst Exploit Video - CVE-2009-1244 – Piotr Bania http://vimeo.com/6595148
- SANS AUD507 http://it-audit.sans.org/courses/description/auditing-networks-perimeters-systems-6
- Vmware Resource Management Guide 5.0 http://goo.gl/rlWbb
- XenServer Administrator's Guide http://support.citrix.com/article/CTX118447
- Hyper-V Security Guide http://technet.microsoft.com/en-us/library/dd569113.aspx
- Hyper-V Attack Surface Reference workbook http://goo.gl/mHJ7J
- Vsphere Security Guide http://goo.gl/7mNUV
- XenApp 6.5 Security Standards and Deployment Scenarios http://goo.gl/EoLSr
- Guide to Computer Log Management NIST http://goo.gl/2h8Zt

Further reading/research

- DEFCON 19: Virtualization under attack: Breaking out of KVM http://goo.gl/oyIGC by Nelson Elhage
- CVE-2011-1751 http://nelhage.com/talks/kvm-defcon-2011.pdf
- **CVE-2012-0217** http://lists.xen.org/archives/html/xen-announce/2012-06/msg00001.html
- http://en.wikipedia.org/wiki/Ring_3
- http://www.linuxjournal.com/article/8540
- http://coewww.rutgers.edu/www1/linuxclass2011/lessons/vmware/x86_challenges.php
- CVE-2012-0217 Immunity Inc POC video http://partners.immunityinc.com/movies/SYSRET-v2.mov
- http://www.pcworld.com/businesscenter/article/257721/vmware_patches_arbitrary_code_execution_flaw_in_desktop_server_virtualiza
- CVE-2012-3288, CVE-2012-3289 http://www.vmware.com/security/advisories/VMSA-2012-0011.html?ClickID=dtzcoxyrhrrybcsmsobmtyorwthhkxnhoybk
- http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-3288

Thank you

rod@hackmiami.info