Cloud Computing Security

Rajendra Kachhwaha
rajendra1983@gmail.com

Feb 13, 2017

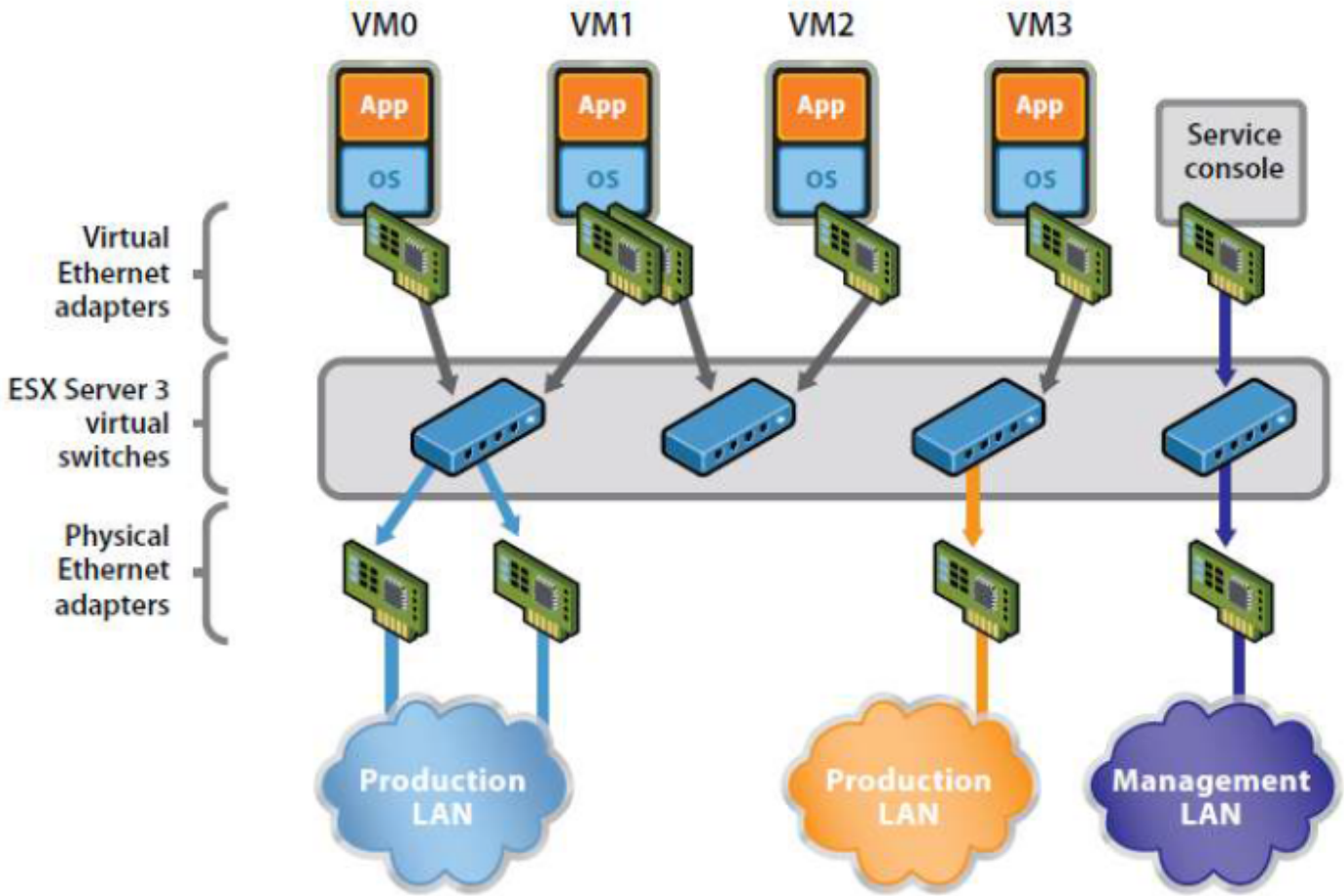
Outline

Example Configuration Issues

1. Virtual machine configuration
   - Resource reservations and limits (for example, on CPU usage) can be established for individual VMs.
     - Allows assignment of more system resources to specific VMs
     - Improper configuration can allow a DoS against one virtual host to affect other hosts on the same server
   - Failure to enable log file rotation can fill disk and DoS the ESX Server
   - Failure to disable unused devices can introduce unnecessary risk

Example Configuration Issues

2. Virtual network configuration: Virtual switches are used to define the topology of virtual networks.



Example Configuration Issues

2. Virtual network configuration
   - Improper configuration can allow unintended communication among guest VMs
   - Network services are enabled to connect virtual machines and kernel services to the physical network
     - Kernel services include features such as virtual machine migration
     - Failure to disable unused services can introduce unnecessary risk
   - VLANs can be used to aggregate multiple virtual switch ports under a common configuration
     - Incorrect aggregation can result in misconfiguration of ports

Hyperjacking

1. Consists of installing a rogue hypervisor
   - One method for doing this is overwriting pagefiles on disk that contain paged-out kernel code.
   - Force kernel to be paged out by allocating large amounts of memory
   - Find unused driver in page file and replace its dispatch function with shellcode
   - Take action to cause driver to be executed
   - Shellcode downloads the rest of the malware
   - Host OS is migrated to run in a virtual machine
2. Known hyperjacking tools: BluePill, SubVirt, Vitriol

Examples

1. CVE-2007-5135:
   (Common Vulnerabilities and Exposures)
   - OpenSSL buffer overflow vulnerability allows remote attacker to execute arbitrary code on the system
   - Affects VMware ESXi server 3.5, presumably the administrative VM (the service console)
   - Involves sending multiple ciphers to take advantage of an off-by one error in OpenSSLs cipher processing code
2. CVE-2009-3760:
   - Remote attacker can write PHP code to Web server configuration script to execute arbitrary PHP code with privileges of server
3. CVE-2009-2267:
   - Guest OS user can gain elevated privileges on guest OS by exploiting a bug in handling of page faults
   - Affects ESX server 4 and other VMware products
4. CVE-2015-4104:
   - PCI MSI mask bits inadvertently exposed to guests.
   - The mask bits optionally available in the PCI MSI capability structure are used by the hypervisor to occasionally suppress interrupt delivery. Unprivileged guests were, however, nevertheless allowed direct control of these bits.

contd.

Examples

4. CVE-2015-4104:
   - Interrupts may be observed by Xen at unexpected times, which may lead to a host crash and therefore a Denial of Service.
   - MSI, Message Signaled Interrupts, uses in-band PCI memory space message to raise interrupt, instead of conventional out-band PCI INTx pin.
   - When system wants to use msi, it should setup msi pci capability control registers.
   - Simply said, it would write address register (32b or 64b) and data register, and set enable bit of msi control register. When device chip wants to send interrupt, it will write the data in data register to the address specified in address register.
   - Using msi can lower interrupt latency, by giving every kind of interrupt its own vector/handler. When kernel see the message, it will directly vector to the interrupt service routine associated with the address/data. The address/data (vector) were allocated by system, while driver needs to register handler with the vector.
   - By allocate vector area generally for all kinds of pci devices, system will reach a general solution to reporting interrupts quickly.
5. CVE-2015-3456:
   - It is a security vulnerability in the virtual floppy drive code used by many computer virtualization platforms.

contd.

Examples

6. CVE-2015-3456:
   - This vulnerability may allow an attacker to escape from the confines of an affected virtual machine (VM) guest and potentially obtain code-execution access to the host.
   - Absent mitigation, this VM escape could open access to the host system and all other VMs running on that host, potentially giving adversaries significant elevated access to the hosts local network and adjacent systems.
7. CVE-2015-2151:
   - Hypervisor memory corruption due to x86 emulator flaw
   - The x86 emulator in Xen does not properly ignore segment overrides for instructions with register operands, which allows local guest users to obtain sensitive information, cause a denial of service, or possibly execute arbitrary code via unspecified vectors.
   - A malicious guest might be able to read sensitive data relating to other guests, or to cause denial of service on the host. Arbitrary code execution, and therefore privilege escalation, cannot be excluded.
8. CVE-2015-0361:
   - Use-after-free vulnerability in Xen allows remote domains to cause a denial of service (system crash) via a crafted hypercall during HVM guest teardown.
   - Malicious or buggy stub domain kernels or tool stacks otherwise living outside of Domain can mount a denial of service attack which, if successful, can affect the whole system.

Examples

1 More CVE

Product	CVE ID	Vulnerability Type(s)	Score	Access	Complexity	Conf.	Integ.	Avail.
Xen	CVE-2015-4104	DoS	7.8	R	Low	None	None	C
Xen	CVE-2015-3456	DoS Exec Code Overflow	7.7	L-N	Low	C	C	C
Xen	CVE-2015-3209	Exec Code Overflow	7.5	R	Low	P	P	P
Xen	CVE-2015-2751	DoS	7.1	R	Medium	None	None	C
Xen	CVE-2015-2151	DoS Exec Code Mem. Corr. +Info	7.2	L	Low	C	C	C
Xen	CVE-2015-0361	DoS	7.8	R	Low	None	None	C
Xen	CVE-2014-9030	DoS	7.1	R	Medium	None	None	C
Xen	CVE-2014-7188	DoS	8.3	L-N	Low	C	C	C
Xen	CVE-2014-3969	+Priv	7.4	L-N	Medium	C	C	C
Xen	CVE-2014-1666	DoS +Priv	8.3	L-N	Low	C	C	C
Xen	CVE-2013-6375	DoS +Priv	7.9	L-N	Medium	C	C	C
Xen	CVE-2013-2211	Other	7.4	L-N	Medium	C	C	C
Xen	CVE-2013-2072	DoS Overflow +Priv Mem. Corr.	7.4	L-N	Medium	C	C	C
Xen	CVE-2013-1432	DoS +Priv	7.4	L-N	Medium	C	C	C
Xen	CVE-2012-6030	DoS	7.2	L	Low	C	C	C
Xen	CVE-2012-3515	+Priv	7.2	L	Low	C	C	C
Xen	CVE-2012-0217	Overflow +Priv	7.2	L	Low	C	C	C
Xen	CVE-2011-1763	DoS +Priv	7.7	L-N	Low	C	C	C
Esxi	CVE-2013-5970	DoS	7.1	R	Medium	None	None	C
Esxi	CVE-2013-3658	Dir. Trav.	9.4	R	Low	None	C	C
Esxi	CVE-2013-3657	DoS Exec Code Overflow	7.5	R	Low	P	P	P
Esxi	CVE-2013-3519	+Priv	7.9	L-N	Medium	C	C	C
Esxi	CVE-2013-1659	DoS Exec Code Mem. Corr.	7.6	R	High	C	C	C
Esxi	CVE-2013-1406	+Priv	7.2	L	Low	C	C	C
Esxi	CVE-2013-1405	DoS Exec Code Mem. Corr.	10	R	Low	C	C	C
Esxi	CVE-2012-3289	DoS	7.8	R	Low	None	None	C
Esxi	CVE-2012-3288	DoS Exec Code Mem. Corr.	9.3	R	Medium	C	C	C
Esxi	CVE-2012-2450	DoS Exec Code	9	R	Low	C	C	C
Esxi	CVE-2012-2449	DoS Exec Code Overflow	9	R	Low	C	C	C
Esxi	CVE-2012-2448	DoS Exec Code Overflow	7.5	R	Low	P	P	P
Esxi	CVE-2012-1518	+Priv	8.3	L-N	Low	C	C	C
Esxi	CVE-2012-1517	DoS Exec Code Overflow	9	R	Low	C	C	C
Esxi	CVE-2012-1516	DoS Exec Code Overflow	9	R	Low	C	C	C
Esxi	CVE-2012-1515	+Priv	8.3	L-N	Low	C	C	C
Esxi	CVE-2012-1510	Overflow +Priv	7.2	L	Low	C	C	C
Esxi	CVE-2012-1508	DoS +Priv	7.2	L	Low	C	C	C
Hyper-V	CVE-2013-3898	DoS Exec Code Mem. Corr.	7.9	L-N	Medium	C	C	C
KVM	CVE-2015-3456	DoS Exec Code Overflow	7.7	L-N	Low	C	C	C
KVM	CVE-2011-2212	DoS Overflow +Priv	7.4	L-N	Medium	C	C	C

Note: C=Complete, P=Partial, L=Local, L-N=Local Network, R=Remote.