SANS ANALYST PROGRAM

Sponsored by Catbird and McAfee

Top Virtualization Security Mistakes (and How to Avoid Them)

A SANS Whitepaper – August 2009

Written by Jim D. Hietala

Introduction

The flexibility and economy of IT resources enabled by virtualization is spawning the rapid adoption of networked server virtualization, which IDC projects will grow to a $20 billion market by 2010.[1] In the past few years, use cases for virtualization have shifted away from early adopters using the technology for software development and testing, toward server consolidation for production environments and critical applications.

Gartner estimates that more than four million virtual servers will be deployed by 2009, and that the number of virtualized PCs will grow from less than five million in 2007 to 660 million by 2011. Gartner also describes virtualization as the highest-impact, trend-changing infrastructure and operation through 2012.[2] Supporting these market projections, a recent SANS survey of over 700 IT professionals that focused on log management issues found that 49 percent of respondents are currently collecting log data from virtual machines, and 68 percent predicted that by 2010, nearly 70 percent of their logs would be collected from virtual machines.[3]

As more virtual machines move into production, organizations are rightly concerned about virtual machine technology being used as a new avenue of attack against them. Their concerns range from finding exploits into important applications running on the virtual machines to the virtual machines serving as a jumping off point into the larger network. Both were proven to be possible at Black Hat in July, when researcher Kostya Kortchinsky demonstrated how to leap from a virtual machine to the host OS and from the host to the virtual machine through two separate memory leak exploits.

In addition to these emerging areas of concern, the foremost problem with virtualization is configuration control. In physical servers, patching and vulnerability management controls are limited to individual physical devices. In a world where IT resources are easily replicated and spun up as virtual systems, there are more demands on configuration management, inventory and capacity management, audit, and training/staffing processes. On the other hand, once we have a solid default configuration and other risk management processes, the management of virtual machine security could actually be carried out more easily in a virtual network than on physical devices and networks because of the virtual network's more centralized controls.

Misconfiguring virtual hosting platforms and guest operating systems is but one of the mistakes commonly made with virtualization. Other common mistakes include poor or lack of patch management oversight for virtualized resources and failure to properly separate duties (in violation of data protection regulations including PCI DSS). This paper explores practical security issues that can arise when virtualization technologies are deployed without proper planning and controls and offers advice on how to avoid making mistakes in critical areas of deployment and management.

[1] Ken Cayton, IDC. "Choosing the Right Hardware for Server Virtualization," April 2008, www.intel.com/business/technologies/IDCchoosingvirthardware.pdf

[2] Gartner Research. "Gartner Says Virtualization Will Be the Highest-Impact Trend in Infrastructure and Operations Market Through 2012," April, 2008, www.gartner.com/it/page.jsp?id=638207

[3] Jerry Shenk. "SANS Annual 2009 Log Management Survey," April, 2009, www.sans.org/reading_room/analysts_program/logMgtSurvey_Apr09.pdf

Virtualization Mistakes to Avoid

Virtualization of IT resources now spans production Web and database servers, storage, and networking. Organizations also need to consider that users may be installing virtual machines on their desktops, as well.

VM technology adds an additional layer to host operating systems that sits beneath the kernel. This layer consists of a stripped down operating system—the virtual machine manager (VMM), such as VMWare's Hypervisor—that manage what can be dozens of virtual machines on a single host. While there are risk areas in the VMMs themselves, most of the discussion in this paper relates to server and networking virtualization security issues and suggestions because that is what IT organizations can control. Beyond accepting vendor patches and keeping VMMs hardened, these virtual machine managers are primarily reliant on vendor support to keep them secure.

Virtual technologies are often used by many of the leading cloud computing platforms and services to provide scalability and deliver cost-effective and dedicated virtual services. This paper doesn't go into detail on cloud security issues. However, the same rules for monitoring, configuration and risk management apply in the cloud. Cloud computing customers must adequately assess security risks (including virtualization issues) posed by cloud services and ensure that necessary controls and access to security- and regulatory-related data within their clouds is accessible when required.

Mistake #1: Misconfiguring virtual hosting platforms, guests, and networks

Creating secure default configurations for virtual machines is much the same as configuring physical machine defaults. In the case of virtual servers, configuration problems are magnified. If a machine build starts out with poor default configurations, including unnecessary ports and services and other such items, those vulnerabilities will extend to each instance of the virtual machine that is replicated from that build.

In light of the virtual machine hacks demonstrated at Black Hat, it is also important to note where virtual applications call to the host and vice versa. Virtual network configuration is another area where organizations make mistakes. On a virtual network, for example, some organizations still host their Web servers and database servers without proper segmentation. Some popular virtualization platforms provide only three virtual switch security configuration settings: promiscuous mode, forged transmits, and MAC address changes. What about when virtual systems make connections to other parts of your network? Moving from virtual to physical switches (and vice versa) makes it difficult to carry over policy and configuration controls between them.

Advice:

Leverage default secure gold builds, then clone other virtual systems from this base. Examples of secure by default configurations are listed at the Center for Internet Security[4] (including benchmarks for popular virtualization platforms) and at the Information Assurance Support Environment.[5]

Manage the virtual machine's configuration lifecycle from cradle to grave with tools native to the virtual machine, and use outside tools where required.

Monitoring tools should be virtual-machine-aware and able to detect and take action (alert/block/sandbox/move to remediation) on assets that deviate from the gold build. They should work with the VMM to correlate changes in VM and virtual network configuration, including on virtual systems behind virtual firewalled switches (which can't be done without working with the Hypervisor/VMM).

Examine closely any virtualization platform capabilities that enable communication between guest and host operating systems, such as device drivers, copy/paste functions, leaks in memory, and so on. Where possible, these should be identified and disabled. System monitoring tools and virtualization-aware monitoring tools should be tuned to locate and monitor these communications paths. In addition, keep an eye on virtualization vendor security advisories for new vulnerabilities and patches.

Mistake #2: Failure to properly separate duties and deploy least privilege controls

Creating separation of duties and providing the least amount of privilege necessary for users to perform their authorized tasks are basic tenets of information security that apply to both physical and virtual resources. Some virtualization platforms collapse the functions of system and network administration so that separating these dutie, is difficult. As such, they give too much privilege and capability to virtual administrators. This level of privilege conflicts with compliance regulations including PCI DSS, FISMA, and others that require separation of duties and least privilege to protect sensitive data. Moreover, high privilege access raises the risk of abuse by privileged insiders, which accounted for 22 percent of breaches investigated by Verizon Business last year, according to the Verizon 2009 Data Breach Investigations Report.[6] Beyond the insider issue, compromise of the virtual administrator's login credentials would yield a powerful set of capabilities for outside attackers.

Advice:

Use tried and true security mechanisms, such as requiring SSH for administrative console access.

Use firewall filter rules to limit administrative virtualization console access to predetermined, authorized, internal network addresses to protect against an outside attacker gaining access to the virtualization administrative console.

Employ a system of checks and balances, with processes to split functions and enforce dual controls for critical tasks. Set up approval processes for creating new virtual machines and moving new applications to new virtual machines.

Monitor and audit logs for virtual machine usage activity in the data center and on end points. Look to VM-aware monitoring tools that can also monitor in non-virtual environments to compare and report per policy. Security tools, such as host-based firewalls and host intrusion prevention, may also prove useful here.

[4] www.cisecurity.com/benchmarks.html
[5] iase.disa.mil
[6] www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

Mistake #3: Failure to integrate into change/lifecycle management

Some specific problems in this category include failure to manage vulnerabilities and patches across virtual systems and failure to conduct system integrity checking for virtual systems. However, with the right combination of controls, organizations may be able to manage their virtual machine lifecycles more easily than their physical environments.

Patch management is an area where virtualization is a mixed blessing. On the negative side, applying patches to the host OS VMM for physical hardware that's supporting numerous virtual systems can cause problems and interruptions with the virtual machines running in production, particularly if a system reboot is required. Of course, a reboot can be done during off hours (just as in the physical realm). And, on the positive side, virtualization can be used to avoid interruption by migrating live applications to other running virtual machines while virtual systems are patched sequentially.

Advice:

The same processes used for events that might trigger patching requirements, including monitoring vendor security advisories, apply in virtual systems. Test patches and follow a change control process.

Look to native management capabilities provided by virtualization vendors as well as third party tools that can scan for vulnerabilities in virtual machines and work independent of and with the VMM (for example to see VMs behind firewalled switches).

Use management agents that are part of default physical server configurations for your virtual servers as well, so that existing change management systems and processes are provided, along with visibility into virtual servers.

Mistake #4: Failure to educate other groups, particularly risk management and compliance staff

Assessment of risk, compliance to relevant regulations, and even software licensing agreements are impacted when new virtual machines can be dynamically spun-up, put to sleep and eliminated. IT auditors, whether internal or external, will need to have a complete understanding of the virtualization infrastructure deployed, the data within the systems, and the policies governing the lifecycle of system instance creation, use, and end of life. Traditional approaches to risk assessment and analysis (sending out assessment questionnaires, analyzing responses) may be inadequate in a virtual environment. If they do assess, some organizations fail to analyze for gaps, so they only assess the obvious and fail to look at interlayered risk areas, such as dependencies on the physical hardware.

Advice:

Educate risk management and compliance groups about virtualization capabilities and limitations. Plan for two-way dialogue regarding evidence collection, what sorts of audit records to create and capture, and other audit and compliance concern areas.

Educate auditors on platform-provided audit/logging capabilities, as well as the ability to create point-in-time system images and snapshots and end of life snapshots. Some third party tools are starting to provide additional capabilities.

Involve compliance staff in critically shaping security policies for the virtual infrastructure in accordance with relevant regulations. An example here might be PCI DSS, where Requirement 7 requires that only authorized users have access to cardholder data, which would require PCI assessors to access virtualization platform audit logs and access control lists.

Review policies and the controls available in the virtualization platform so that compliance staff and auditors fully understand access control capabilities and settings. Explain any additional third party controls as well. Put these control areas in context of data types in the virtual systems that need audit and controls.

Assess and analyze risk at the onset of new virtualization projects, and keep risk management staff involved with (and give possible sign off to) changes in the virtualization infrastructure that can affect the risk posture.

Be prepared for massive storage requirements!

Mistake #5: Lack of availability or integration with existing tools and policies

Reinventing the wheel is costly and often not necessary. However, many common defense-in-depth practices used in securing physical servers (hardware firewalls to create security zones for sensitive applications and data, intrusion sensors to inspect network traffic, and so on) are unavailable (or at best extremely hard to configure) in virtual environments. This is because the data is traversing a system backplane, not an IP network.

To the extent it is possible to use physical security devices with virtual servers, careful virtual network configuration is required to redirect and force traffic through an external switch fabric and security infrastructure. It's also a mistake to assume that hardware security tools that work in physical environments work smoothly in virtual machine environments. Even if they can be used, the complex virtual network configuration required can cause other security issues; for example, if virtual machines fail or require maintenance and applications have to be moved.

However, it's also a mistake to leave existing tools out of the equation. With virtualization becoming ubiquitous, security and network management vendors are working to make their tools virtual-aware. Your current provider, for example, may have plans for virtual coverage on its roadmap. Some providers may already have degrees of virtual-aware capabilities, and what they don't have, they're partnering with other vendors to accomplish.

Advice:

Emulate standard security software on your virtual machine instances, including anti-malware, host intrusion prevention, endpoint security software, and host firewalls.

Don't assume that all new tools are required to manage your virtual environment: Many traditional security and management vendors are rapidly adding functionality that can address virtualized resources, so check with your current vendor or reseller.

Evaluate options for deploying key security functions, including system and file integrity tools, intrusion prevention systems, firewalls, and others, as virtual appliances. These tools provide the same control capabilities as their physical counterparts, but in a virtual form factor.

Evaluate in-use security solutions for capability in virtualization scenarios. Check with your reseller or security vendor partner about their roadmap; look for partnerships that would enable maximum coverage with minimal change to your infrastructure.

Mistake #6: Lack VM visibility across the enterprise

VM sprawl is a general term describing the propagation of virtual systems across the enterprise in an uncontrolled way. Rogue machines can consume resources and bandwidth as well as present new vulnerabilities with virtual machines that are not being patched and monitored. Forensics cannot be conducted in the virtual environment in which these machines aren't even visible to the organization. Should an event occur, organizations need to not only know what part of the network is affected, but also be able to roll back network and system records in time to determine what happened.

Just as discovery of physical IT assets is necessary (and challenging), discovering virtual systems (and the applications running on them) is equally important and challenging. On one hand, there are more machines concentrated in one place (presumably as monitored data center servers) so that should make visibility easier. But those machines are moving around between users, and rogue machines are being installed on end points. Furthermore, the capability for attackers to counterfeit machine installations is not too far off. Because each virtual machine has browsers, ports and other open doors to malware, it's critical that each machine and connection is discovered and put under controls that would include roll back capability in case a compromise occurs.

Advice:

Existing security tools such as network mapping and scanning systems may be able to provide some asset discovery for virtual machines, but may not be able to see past a virtual firewall switch. Look to virtual-aware technologies that can do asset discovery, port mapping and application inventory for virtual machines and network devices. It would be most helpful if these tools can also provide network mapping for interdependencies among virtual machine networks, their host, and VM network extensions to the physical network (switches/routers and other such devices).

Integrate virtual machines into existing system lifecycle processes. This, too, may require new VM-aware tools that work in conjunction with the management capabilities in the VMM to see beyond secure network segments.

Mistake #7: Failure to work with an open ecosystem

Flexibility for expansion and the ability to tie together separate components of virtualization security for management is crucial to getting our arms around the full array of virtual machine risk areas. In the relatively new area of virtualization security, organizations are faced with the traditional point products targeting singular problems that should, ultimately, be managed in a larger ecosystem. Until the market matures and integrates, virtual security will require the help of more than one vendor, which makes interoperability an issue. It is likely we'll see organizations turning toward platforms in which larger security and network management framework vendors are partnering with virtual niche vendors to offer the most coverage.

Advice:

Look for best of breed capabilities that have the best chance of meeting your risk management, audit, and integration needs, while working with your existing infrastructure through partnerships and standards. An example of an emerging standard that is worth following is SR-IOV (single root, I/O vector) from the PCI SIG . This standard will enable binding of security policy to virtual machine images.

Look for complementary virtualization security tools that integrate or can be fashioned to work together or as a part of a collaborative ecosystem. Standards will ultimately improve security capabilities and interoperability.

Mistake #8: Failure to coordinate policy between virtual machines and network connections

With physical systems and network connections, we can be fairly sure that once we establish policies and physically connect servers, routers, switches and network security devices, things will remain static and change control policies will govern how policy and network configurations may be changed. It's the opposite with virtualization, which makes the creation and movement of virtual machines highly dynamic. This dynamic nature is the beauty of virtualization, but it is also problematic when it comes to attaching and enforcing security policy for virtual machines as they are moved around.

VMs can also be modified in ways that their physical counterparts rarely would. Changes to network interfaces and port-group memberships can be made quickly and can therefore easily undo established network security zoning. The kind of isolation and security zones created through the use of firewalls, routers, switches, IPS devices, and other such physical devices on the network can be created in virtualization environments. The trouble is in getting the rules to follow the virtual machines as they move around.

In addition, providing access control protections for the host OS platform is a highly desirable defense-in-depth strategy that can be achieved through the use of tools such as TCP Wrappers, pluggable authentication modules (PAM) and iptables. These technologies can provide access control capabilities for the virtualization host, allowing access control by hostname, IP address, time of day, group membership and username.

Advice:

Use security policy management tools, along with processes governing the management of virtual machines, to ensure that changing the location of VMs will trigger replication of required security functions to the new location.

Ensure that physical infrastructure such as routers and switches, or their virtual environment equivalents, are bound to virtual machines. Create policies that move network associations required for virtual machines around with the virtual machines themselves. Seek virtualization-aware solutions that can help manage network security policies and work with the VMM/Hypervisor for added visibility and control.

In the longer term, look for integrated and virtualization-aware solutions to more tightly couple security functions to virtual machines. Standards such as SR-IOV, mentioned earlier, will help make this a reality because they allow network security policy and capability to be bound to virtual machines.

Mistake #9: Failure to consider hidden costs

At first glance, server consolidation through virtualization promises immense savings in hardware, software and administration. However, don't make the mistake of underestimating the new cost areas introduced by developing and managing a virtual infrastructure. New expenses may include (but are not limited to) security and audit, configuration/lifecycle management, inventory and capacity management, and storage. Consider other costs like training operations and security staff on the new infrastructure; purchasing the new products required for moving security, risk management, audit and operational controls (including secure failover); licensing; and the potential costs failing to meet regulatory requirements. Some virtual configurations may require the deployment of more virtual security appliances—at potentially greater cost than similar physical configurations. In addition, some vendor pricing models for software will need to be changed, including those for software security products.

Advice:

Study your requirements against your existing infrastructure and future virtualization plans to maximize your investment. Work with partners and resellers to leverage their experience and knowledge of your network.

When adding VM security management tools and processes, consider soft cost elements such as training, integration time, internal support and maintenance.

Consider licensing costs, vendor-provided service agreements, roadmaps and partnership plans in relation to the provider's virtual coverage.

Mistake #10: Failure to consider user-installed VMs

User-installed VMs have not been seen as a big problem to date, but given the growth projected in endpoint virtualization, it almost certainly will be. In many ways, security for virtualization on the end point will be the same as with server virtualization. However, advanced end users with virtual machines may have special requirements for configuration and patch management. There are also questions regarding how central IT staff will recognize the existence of VMs on endpoint systems; how they will control the use of these technologies by end users; and how licensing and patching issues can be resolved around desktop applications on virtual endpoints that may be operated by unsophisticated users.

Advice:

Rootkit and malware installers already have VM-aware capabilities. At Black Hat in July, it was demonstrated that a malicious or infected VM can be used to jump to the host operating system and own the host and all the virtual machines on it, which could, then, lead spread out to the physical network. As a result, it is critical to have an internal usage policy and network and endpoint security that is VM-aware enough to locate and identify virtual machines and report them.

A new set of management capabilities may be needed that allows IT desktop support, security operations, and help desk staff to discover virtualization in use throughout the organization's endpoints, set and monitor policy, and have visibility into the status of virtual machines running on desktop systems. Asset discovery for virtual systems running on endpoints is a capability that endpoint security management solutions will need to develop to enable this visibility and control.

Summary: Looking Forward

The usage of virtualization in cloud computing services is another trend that bears watching. From a security operations standpoint, there are new wrinkles introduced by these scenarios. One example is patch management responsibility. In a Platform- or Infrastructure-as-a-Service cloud scenario, responsibilities for patching operating systems and applications for virtual servers may be split. As an example, the cloud service provider might have some responsibility for patching operating systems, and the customer organization might have responsibility for patching applications. Ensuring that needed patches are applied in a timely manner will require close coordination and service level agreements spelling out expectations for things such as patch frequency, maintenance windows, and acceptable intervals from vendor patch availability to service provider or customer patch deployment.

Tighter integration of security capabilities is also in the future. Virtualization platform providers have introduced APIs, thus allowing security technology vendors to more tightly integrate their security capabilities as virtual appliances. While this is a positive development, there are caveats. First, in many large enterprise environments, security technologies have been engineered and optimized to provide high throughput, low latency, and high availability with failover capability. When run in virtual machines, the high availability/failover aspect is immature at best. Inventory and capacity management rules will have to be set and followed in the virtual machine environment wherein many virtual resources are drawing off a single host. It isn't clear that general purpose server hardware will deliver on the throughput and latency expectations.

Security technologies are rapidly evolving to address the unique issues posed by running virtual machines. While some security technologies are not yet optimized for use in virtual environments, many can help achieve security objectives. Going forward, virtualization-aware security technologies should provide the visibility, control, and the level of integration with virtual systems that will deliver a secure and manageable environment—possibly more so than in the physical system environment.

About the Author

Jim Hietala, GSEC, CISSP, is vice president of security for The Open Group, where he manages all security and risk management programs and standards activities. He is also the research director and a principal of the Compliance Research Group, providing research, analysis and consulting services in the areas of compliance, risk management, and IT security. Hietala has provided research and consulting services to numerous organizations. He is a frequent speaker at industry conferences, and he recently authored a comprehensive course on IT risk management. He is a regular contributor to the SANS Analyst/Expert program and to the Cloud Security Alliance as a reviewer for the Governance and Enterprise Risk Management domain (version 1 guidance) and as a leader of the Compliance sub-domain (version 2). His articles have appeared in the ISSA Journal, Bank Accounting & Finance, Risk Factor, The Compliance Authority, Cutter IT Journal, SC Magazine, and others. An industry veteran with more than 20 years of IT security experience, he has held leadership roles at ControlPath, Avail Networks, Alternative Technologies, eSoft, Qwest, Concentric Network, and Digital Pathways. He developed and launched the industry's first remote access VPN service (Concentric RemoteLink) and encrypting ISDN router (Network Express), and he has launched two compliance and risk management software startups into the IT-GRC market. He holds a B.S. in Marketing from Southern Illinois University.

SANS would like to thank this paper's sponsors