Interested in learning more about security?

SANS Institute InfoSec Reading Room

IT Audit for the Virtual Environment

SANS ANALYST PROGRAM

Sponsored by VMware

IT Audit for the Virtual Environment

A SANS Whitepaper – September 2009

Written by: J. Michael Butler and Rob Vandenbrink

Introduction: It All Boils Down to PII

Similarities and Differences

Practical Applications

Introduction: It All Boils Down to PII

Industry requirements, government agency directives, and federal and state disclosure laws (starting with California's SB1386) have one goal in common: **Protect personal and private information**. It really doesn't matter whether we are talking about credit card information, bank account numbers, social security numbers, health data or insurance information. In fact, instead of personal information, some organizations are focused on protecting utility infrastructures, such as power plants, telecommunications, or gas lines. Although the information requiring protection in such a case is not "personal," the same security and audit principles still apply.

So, to achieve compliance, IT groups check policies and procedures against rules, regulations, and directives. They follow best practices and build defense-in-depth. IT auditors, SAS70 auditors, and PCI QSAs (Qualified Security Assessor) meet with the operations teams, whose responses show that they are, indeed, compliant…that is, until we start talking about virtualization. In this realm, auditors are usually at a loss.

Virtualization is gaining popularity because of its promise of increased return on investment (ROI) by reducing the data center footprint and power requirements. Gartner estimates that more than four million virtual servers will be deployed by 2009, and that number will grow to 660 million by 2011.[1] According to a recent SANS Log Management Survey of more than 700 IT professionals, 49 percent of respondents are currently collecting log data from virtual machines, and 68 percent of those predict that, in 2010, nearly 70 percent of their logs will come from virtual machines.[2]

As organizations move ahead with their virtualization programs, they need to understand the security and audit implications in the layers and features presented by virtual machine farms, and their VMMs (virtual machine managers).

For starters, virtualization introduces a new layer known to most as Hypervisor, which is VMware's virtual machine manager. Virtualization also creates a new environment in which virtual machine systems—connected via virtual network interfaces, virtual routers and virtual switches and traversing virtual network paths—are dynamically moving around. In addition, virtualization introduces new storage considerations around virtual drives, network storage systems and fiber channels.

[1] 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

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

All these new layers, devices and traffic require management and protection just as they would if they were physical machines and networks. But what do auditors need to know in order to successfully locate and ensure secure processes around sensitive data traversing this new virtual environment?

Unfortunately, at this early stage of adoption, there is little guidance within the regulatory frameworks on how to address new audit issues presented with virtualization. The purpose of this paper is to help IT managers and auditors come together and understand the virtualization process and the new risk and audit areas this technology presents. It also offers guidance on developing audit review processes that can be applied to virtualization, including how to use virtualization to enhance audit processes.

For purposes of brevity, this paper will focus on PCI DSS audit in a VMware environment, which is currently the most widely used virtualization platform. VMware's own reports claim that its ESX development platform is in use by 95 percent of the global fortune 500 companies.[3] According to CNN in January of this year, VMware had captured 85 percent of the market for all virtualization implementations.[4] Although these principals are VMware and PCI DSS specific, they can be applied to most regulations/mandates, as well as to most enterprise virtual environments.

[3] www.vmware.com/technology/whyvmware/virtualization-customers.html

[4] money.cnn.com/2009/01/19/technology/shambora_vmware.fortune/index.htm

Similarities and Differences

Virtual machines need to be secured and audited exactly as they are in physical network-server environments. Such measures include the familiar procedures and checklists that we've used all along: System hardening and security, change control, blocking of unauthorized equipment and applications, network segmentation, monitoring, logging, alerting, and documentation that supports audits of these processes.

The benefit of auditing in the virtual world is that virtual server farms are more centralized and therefore more easily managed. As an example, PCI DSS addresses configuration and change control applied to initial and final configurations. Because VMware is easily auditable using scripts, audits for change can be done periodically, perhaps daily, with alarms to trigger on configuration changes. These changes can then be compared to documentation indicating what changes have been approved, and can also verify that approved changes occurred in agreed upon maintenance windows.

There are many tools available to audit change control in a virtual infrastructure that will generally audit against the main regulatory framework requirements as well. They also include their view of compliance to several frameworks, including: VMware Hardening Guide, PCI-DSS, SOX, HIPAA, GLBA and ISO 17799 (in short, most frameworks except for JSOX).

In addition to commercial tools, VMware offers APIs and command line tools to permit audit operations from Perl scripts from the ESX Service Console or vSphere command line interface. Audits of overall environments are generally carried out using the Powershell APIs against the vCenter "view of the world." Audits using these tools can capture not only many of the ESX specific controls, but also the controls that are only seen from vCenter, such as the impact of VMotion (migration), HA (high availability) or FT (fault tolerance) on compliance or separation of duties enforced through permissions on user accounts. However, some controls are best assessed from the ESX hosts themselves. ESX Firewall settings, for instance, are not always accurately reflected in the vCenter console, and should be assessed both from vCenter and from the host itself (using the "esxcfg-firewall" command).

Finally, most of the information that is required for audit purposes is available by manually navigating the vCenter console. However, there are two challenges in using this approach: repeatability and formatting. Manual approaches to audit must be backed up with stringent, documented manual processes to ensure that successive audits are actually assessing the same controls in the same way. More important, collecting audit information manually forces auditors to create and format their audit from scratch, often manually transcribing information from a GUI screen or in some cases relying on graphical screenshots. Such procedures can result in errors and/or changes in audit metrics as the GUI changes across versions. Moreover, the manual procedures add significantly to the time required to assemble an audit, when compared to basing an audit on text-based information collected and preformatted by commercial audit tools or script-based toolsets.

Practical Applications

Practical applications of audit in virtual environments may vary depending on configuration and interoperability issues. Despite these environmental differences, audit programs should contain the following control areas:

Audit and Infrastructure Planning

The single largest issue with respect to PCI compliance is separation of virtual servers and devices—and further separation from the guest operating system (i.e., PCI section 2.2.1). Separation of virtual server, switches, port groups on virtual switches, and separation of the guest operating systems from the service console are clearly defined in the VMware Virtual Infrastructure.

However, these things are not spelled out in any current regulatory framework. This ambiguity means that the easiest approach for auditors is to take the word "separate" to mean "separate hardware," and simply insist on separate servers or a separate physical servers to house data that falls under PCI requirements. With proper segmentation, configuration and controls, however, separate hardware should not be necessary.

PCI auditors often recommend PCI VLANs rather than separate hardware, because VLANs are well understood by the QSA community. A PCI VLAN is considered by most to be a "separate enough" network segmentation technique between virtual server farms, so long as the VLANs can pass tests to indicate that appropriate controls are in place. Hopefully, the next version of the PCI-DSS framework will offer a similar approach toward virtualized infrastructure segmentation.

It is important, however, to ensure that PCI compliance is maintained when the more advanced features of virtual infrastructures are employed. For instance, VMotion, high availability (HA), fault tolerance (FT), distributed resource scheduling (DRS), distributed power management (DPM), and even basic system administration programs all have the ability to move a host to a different network segment. Any of these moves can change the security posture of a host and its associated PCI-governed data.

The PCI committee on virtualization is working on security guidance for virtual environments that may be inserted in the next version of the PCI standard. Currently, however, such guidance does not exist. If your company is planning a substantial financial or project outlay for a virtual infrastructure, it's a good idea to involve a QSA (preferably your regular auditor or audit firm) provide a written opinion on the infrastructure as part of the design process.

Configuration

It is a common practice to create new virtual machines from gold images. These are VM images that are completely installed and customized to a particular environment and security standard, which promotes a consistent, auditable server environment. However, there is a hidden risk in this approach, which is the potential for misconfiguration of servers and systems as they replicate, spin up, spin down and move around in the dynamic virtual environment. Standard update mechanisms (auto-update from the Internet or from internal corporate update servers) will apply patches. However, mandated configuration updates are often applied in a catch-as-catch-can, out-of-process manner, resulting in non-uniform server builds.

Change control procedures should be updated so that changes affecting servers are also applied to their base images. This keeps all images in sync with current security and operational requirements and is as simple as adding a field to the change control form to ensure that this step isn't forgotten. For auditors, the process should be requested and verified. It's also a good idea to go back and identify a few recent updates in change control to verify that the changes have been applied to relevant gold images.

Auditors must take similar steps with Hypervisor, ensuring the existence of a hardened, gold build of Hypervisor, and then documenting how it has been managed and maintained with updates, patches, audit logs, and alerting/reporting of changes.

Network configuration must also be controlled and maintained. Here, the vCenter interface allows for logical naming schemas for network segments, servers and storage infrastructure components. This allows organizations to construct a self-documented infrastructure, where components that fall under PCI regulations are clearly identified by name in every administrative view within vCenter. If implemented, this approach of naming components also makes auditing for compliance easier, as the map views within vCenter show the relationship between the various PCI components in the infrastructure.

Visibility

This mapped view into the PCI components of the infrastructure is one of the major security benefits of virtualization. The Hypervisor administration console (vCenter in the case of VMware) gives the administrator full visibility into network, storage, resource management and administrative configuration. The Map View within vCenter gives the auditor a complete picture of virtual machine connectivity to the virtual network and virtual storage infrastructures, as well as any separation required for PCI Compliance. vCenter also grants a common interface for several operational tasks, including logging, performance and resource utilization, and overall utilization of storage. This bird's eye view of the data center is simply not possible in a traditional data center with connections between physical devices.

Separation of Duties

By default, the VMware administrator has full rights to all activities in the infrastructure. In many cases (particularly in smaller environments), this default is not changed during setup and use. Worse, this level of full rights access is copied into mirror images and all other aspects of the virtual machines within the data center. Where the default permissions are not changed, then, a single breach of the administrator's access could lead to an attacker gaining full ownership of the entire server farm.

In addition, failing to change the permissions configurations makes the phrase "who watches the watchmen?" very relevant in this case. So, it is incumbent on the IT group to properly implement change control, separation of duties, configuration management, and proper logging to mitigate this exposure. Using the vCenter interface, some of the following separation of duties (SOD) options can be achieved:

- Server administrators can be given power on/power off rights to their own servers and no others.
- Network administrators can be granted the rights to patch servers into virtual switches and create virtual switches.
- VMware administrators can be granted the rights to deploy new VMs but not to modify existing VMs.
- Auditors can be given view-only rights to all configuration information in the infrastructure.

If implemented correctly, SOD in the virtual network server environment can be enforced at a technical level that is not possible in the physical environment. For instance, in the physical world, a network administrator could press the power button on a server, or a server administrator could patch his or her server into a network switch. In a virtual world, both of these activities can be denied with technical controls.

Storage Virtualization

Storage virtualization has been common in data centers for decades. Local storage virtualization (commonly RAID) does not generally have a significant impact on PCI and other regulatory frameworks. However, every other virtualization method of storage infrastructure certainly does.

Fiber Channel is generally viewed as the premier storage mechanism and is present in almost all data centers. However, performance in Fibre Channel is almost always at the expense of security. Even though assisted encryption is an option in many HBAs (host bus adapters), it's rarely implemented for performance reasons. As a result, Fibre Channel data is almost always transported in clear text.

Because of this, Fibre Channel architectures are susceptible to attacks of several types that are analogous to attacks in the physical Ethernet world, including session hijacking and man-in-the-middle attacks. WWN (world wide name) spoofing in Fibre Channel corresponds to MAC address spoofing in the Ethernet world, while zone hopping is very similar to VLAN hopping on Ethernet switches. LUN (logical unit number) masking attacks are simply a variation on WWN spoofing viewed from the storage processor rather than the HBA perspective.

Other types of transport also communicate in plain text. iSCSI (Internet small computer storage interface) and NFS (network file system) are almost always transporting data in clear text on the virtual network. A successful man-in-the-middle attack will often target the data itself, but iSCSI credentials offer an interesting alternative. Because iSCSI uses simple CHAP (Challenge Handshake Authentication Protocol), once the credential hash is captured, the actual credentials are not required to impersonate the supplicant host and hijack the session. This is often called a "Pass the Hash" attack.

For these reasons, both iSCSI and NFS are generally implemented on dedicated VLANs or dedicated storage networks. Documentation, change control, and configuration management are all good approaches to mitigation of risks in storage virtualization.

Network Virtualization

Network virtualization is another infrastructure that should be considered in the context of audit, compliance and security. There are two main virtual networks to consider: Virtualization of the LAN using VLANs, virtualizing the WAN using MPLS (multiprotocol label switching) or frame relay (in older WAN infrastructures).

VLANs offer excellent local network segregation as required in the PCI specification, and are often recommended by auditors because they are easily implemented and offer a cost-effective alternative to a dedicated switch for PCI services. In fact "PCI VLAN" is a common industry term. However, care should be taken when implementing VLANs for segregation. Traditional VLANs are often susceptible to nested VLAN attacks, which involve using double-encapsulated 802.1q frames to jump from one VLAN to another (for instance, from a general purpose VLAN to a PCI VLAN). In addition, a simple misconfiguration—an error in an ACL (access control list) for instance—can expose data.

Cisco and other switch vendors have excellent documentation on remediation for the issue of "VLAN jumping," but there is simply no substitute for care in configuration followed by periodic penetration testing using a variety of commercial tools available for virtual machine environments.

It's also important to note that VMware's virtual switch implementation is not susceptible to many of the common VLAN and other layer 2 attacks. This point is often overlooked in conversations with auditors, so it is important to specifically bring this information forward.

The more common risk in these virtual network infrastructures is misconfiguration. It is not uncommon to have a link to a remote office unavailable on a Monday because maintenance was done on Sunday and a router was rebooted without saving its running configuration. These "Monday ops OOPS" situations have been common for as long as there have been WANs. What most people do not consider in such update and repair situations is that the run link is still connected to something. It may be connected to an unswitched segment or to some other customer's network—a situation not commonly detected. This is, in effect, reclassifying the WAN network from a trusted network to an untrusted network, which invokes the PCI rules to encrypting data in transit over the untrusted segment.

The technical control that can mitigate both misconfiguration and malicious attacks is to encrypt virtual WAN data using a strong algorithm over the MPLS or other WAN. Also, secure your WAN interfaces using ACLs, permitting only encrypted traffic.

[5] "VMware vSphere Online Library, Virtual Switch Protection and VLANs." http://pubs.vmware.com/vsp40_e/server_config/wwhelp/wwhimpl/common/html/wwhelp.htm#href=c_virtual_switch_protection_and_vlans.html (accessed August 2009).

Disaster Recovery

Disaster recovery is an area that can easily benefit from the use of virtualization to create spontaneous rollover capability to offsite storage. Business continuity planning is all about preparing for disasters so business operations are maintained during a disaster, so, during this planning, organizations can lose sight of security and compliance requirements. For instance, it is very common to see all critical hosts replicated or restored to a single virtual infrastructure without the separation that is required for PCI compliance.

Disaster recovery (DR) operations, by their nature, involve the most confidential and sensitive data and most essential processes in the corporation. Some virtual audit program requirements to consider in disaster recovery planning include:

- The production firewall, intrusion prevention and IPS posture should be maintained at the DR site. If the firewall rules are different (i.e., the firewall rules are not enabled until a disaster is declared), then the DR firewall should be audited regularly.
- Change control should be implemented such that the DR site and the primary site are kept in lock-step. The last thing you want is a breach because the DR firewall hasn't been patched or updated since it was installed.
- Log monitoring for the DR site should be treated with the same rigor as the primary data center. Do not try to save on SIM licenses by not covering your DR site! The last thing you want is to have a breach and totally miss the incident.
- The DR site should be audited and pen-tested as an entity separate from the primary site, with the same frequency and rigor.
- Finally, replication to the DR site should be encrypted.

Summary

As studies and statistics show, virtualization is already upon us. But along with the cost savings and smaller footprints offered by virtualization, there are new security, management and audit responsibilities that must be addressed. The same audit obligations for hardware environments must now be applied to virtual networks. However, there are also many new audit program areas to incorporate as a result of virtualization—visibility, configuration management, network management, disaster recovery, and more.

There is no clear contractual, regulatory or legal guidance as to how to secure and audit in a virtualized environment. So organizations need to align their virtualization projects with audit procedures before these virtualization requirements are defined. When it comes to achieving and documenting compliance, tools native to the virtual machine products offer a good starting point.[6] Commonly used third party tools that have done a good job with audit controls in the physical world are also adding value to the virtualization audit process.

Ultimately, security and IT staffs should be working together to continually assess the audit/risk areas introduced by virtualization. With proper program guidelines and controls, virtual machine networks should be easier to monitor and document for auditors because of the more centralized nature of virtual machine farms and the management capabilities provided natively and through third party tools.

[6] An example for VMware:
www.vmware.com/files/pdf/vi35_security_hardening_wp.pdf

About the Author

J. Michael Butler, CISA, GSEC, EnCE, GCFA is an information security consultant with LPS, a leading provider of computer services to the mortgage industry. Butler's responsibilities have included internal audit of information systems and infrastructure, information security policies, (aligned to ISO and addressing federal and state disclosure laws), enterprise security incident management planning, computer forensics, service delivery, and distributed systems support. He has also been involved in authoring SANS security training courseware, position papers, articles, and blogs. Butler has more than 27 years of experience in the computer industry.

Rob Vandenbrink, MSISE and GIAC advisory board member, is coauthor and instructor of the SANS Institute's comprehensive course titled "Virtualization Security and Operations." Since 1981, he has worked in all facets of networking and security, and has been a consultant at Metafore (www.metafore.ca) since 1994. Vandenbrink's practice covers international clients in the financial, manufacturing and healthcare sectors. His current projects and interests include Powershell automation of VMware, VMware security, scripting on Cisco IOS, and security in Fibre Channel architectures, among other areas. He holds a Bachelors degree in mechanical engineering from University of Waterloo and is working toward a Masters degree in information security at the SANS Technology Institute (www.sans.edu).

SANS would like to thank this paper's sponsor:

Last Updated: May 28th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Madrid 2017	Madrid, ES	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GAUS	May 30, 2017 - Jun 04, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CAUS	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DCUS	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TXUS	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Milan 2017	Milan, IT	Jun 12, 2017 - Jun 17, 2017	Live Event
SEC555: SIEM-Tactical Analytics	San Diego, CAUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NCUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, NL	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, COUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MNUS	Jun 19, 2017 - Jun 24, 2017	Live Event
DFIR Summit & Training 2017	Austin, TXUS	Jun 22, 2017 - Jun 29, 2017	Live Event
SANS Paris 2017	Paris, FR	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, AU	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MDUS	Jun 26, 2017 - Jul 01, 2017	Live Event
SEC564:Red Team Ops	San Diego, CAUS	Jun 29, 2017 - Jun 30, 2017	Live Event
SANS London July 2017	London, GB	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, JP	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, SG	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CAUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS ICS & Energy-Houston 2017	Houston, TXUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, DE	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DCUS	Jul 22, 2017 - Jul 29, 2017	Live Event
Security Awareness Summit & Training 2017	Nashville, TNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, ILUS	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, AU	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Stockholm 2017	OnlineSE	May 29, 2017 - Jun 03, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced