Virtualization Security Checklist

This virtualization security checklist is intended for use with enterprise full virtualization environments (as opposed to paravirtualization, application or operating system virtualization) most commonly used in servers, with so-called bare metal virtualization (i.e., Type 1) and with hosted full virtualization (i.e., Type 2). (This checklist does not cover desktop virtualization or cloud service provider environments.) This checklist is also intended to be product and vendor agnostic to provide the broadest coverage possible about full virtualization security issues. As such, users are strongly encouraged to consult relevant vendor and product documentation for specific implementation information applicable to these recommendations.

Recommendations listed here are guidance, and do not connote sufficiency for specific environments and implementations. An explanation of terms used in this checklist is found in Appendix A, Glossary. Users are encouraged to review these recommendations with their information security and audit personnel. These recommendations are drawn from multiple sources in an attempt to be as comprehensive as possible, without being vendor or product specific. A complete list of sources consulted is found in Appendix B, Sources.

This checklist is divided into the following sections:

1. Securing the virtualization platform

a. Platform and installation requirements

1.a.1 Limit physical access to the host: only authorized administrative personnel should have physical access to the host system to prevent unauthorized changes.

1.a.2 Verify integrity of files prior to installation: verify the hash values of system files, as provided by the vendor, prior to installation to ensure integrity.

1.a.2.1 Hash values should also be stored separately offline (e.g., on a CD-ROM or other read-only media) to ensure that a malicious user has not re-hashed any modified files.

1.a.3 Load and enable only required operating system components and services: no unnecessary operating systems components (e.g., drivers) should be loaded, and no unnecessary services should be enabled (e.g., printing services, file sharing services).

1.a.4 BIOS, bootloader passwords: passwords should be used for BIOS and bootloaders (e.g., GRUB) for both hosts and guests.

1. Securing the virtualization platform

b. Privileged partition operating system hardening

1.b.1 Limit VM resource use: set limits on the use of resources (e.g., processors, memory, disk space, virtual network interfaces) by each VM so that no one VM can monopolize resources on a system.

1.b.2 Ensure time synchronization: ensure that host and guests use synchronized time for investigative and forensic purposes.

1.b.3 Minimize number of accounts: hosts should have accounts necessary for managing VMs only. Use of strong authentication (e.g., two factor authentication) is recommended, but if passwords are used then ensure that they are strong, hard to guess, changed frequently, and only provided to authorized administrators. Credentials used for access to the host OS should *not* also be used for access to guest OSs.

1.b.4 Unnecessary programs and services: all unnecessary programs should be uninstalled, and all unnecessary services should be disabled. This action not only improves security, but will likely improve system performance as well.

1.b.5 Configuration management: configuration management of host OSs should be centralized to ensure that configurations are standardized. It is likely that multiple configurations will be required to meet business needs (e.g., high risk, medium risk, low risk, etc.), but deployed configurations must be documented in order to be effectively managed.

1.b.6 Patch management: host OS must be patched regularly and in a timely fashion to ensure that the host OS is protecting the system itself and guest OSs properly. In addition, the same patching requirements apply to the virtualization software. This patch management is, obviously, important for systems' security. However, timeliness includes procedures for testing patches on non-production systems first to ensure that access to VMs is not disrupted.

1.b.7 Hardening guide: host OS should be hardened following an organization's approved hardening or build standard, which can be developed from independent guides (e.g., the Center for Internet Security, Defense Information Systems Agency, National Security Agency), or from vendor guidance.

1.b.8 Administrator or root login: no authorized administrators should be authorized to login to systems as “administrator” or “root”. Instead, authorized administrators should login with their own accounts, either set-up with sufficient administrative rights (e.g., using sudo), or *su* to “root”.

1. Securing the virtualization platform

c. Partitioning and resource allocation

1.c.1 Space restrictions: volumes or disk partitioning should be used to prevent inadvertent denials of service from virtual machines (guest operating systems, OSs) filling up available space allocations, and allow role-based access controls to be placed individually on each virtual machine (guest OS).

1.c.2 Disconnect unused physical devices: individual VMs can be configured to directly or indirectly control peripheral devices attached to the host system. VMs should be configured by default to disable such connections. Connections to peripheral devices should be enabled only when necessary.

1.c.3 Virtual devices: ensure that virtual devices for guest OSs are associated with the appropriate physical devices on the host system, such as the mapping between virtual network interface cards (NICs) to the proper physical NICs.

1.c.4 Use of virtual trunk ports: physical switch ports connected to virtual trunk ports should always be configured as static trunk links. A virtual switch cannot connect to another virtual switch or to more than one external physical switch. For that reason, physical switch ports connected to virtual switch trunk ports should always be configured as static trunk links and spanning tree protocols should be disabled. (A virtual switch might not support topology discovery or dynamic trunking protocols, such as Cisco PVST+. That is because virtual switches might not have a need to detect connected network devices.)

1.c.5 Use Layer 2 security configurations: Layer 2 security policies provide enhanced network security for virtual networks by restricting the ability of virtual adapters from entering promiscuous mode and examining all switch traffic, placing frames with a forged MAC on the network, and changing of their own MAC address in order to intercept traffic destined for a different virtual machine.

1. Securing the virtualization platform

d. Administration and management

1.d.1 Strong authentication should be used for host system access: two-factor authentication is recommended for access to host system.

1.d.2 Do not enable file sharing between host and guest OSs: while it might be convenient to enable the sharing of system files between the host and guest OSs, allowing such introduces an unacceptable risk of a guest OS possibly maliciously changing a host OS file.

1.d.3 Warning banners: warning banners should be used for both hosts and guests. Warning banners are required to successfully prosecute unauthorized users who improperly use a computer. Banners should be displayed on all systems prior to access and warn users about: (a) what is considered the proper use of the system; (b) that the system is being monitored to detect improper use and other illicit activity, and; (c) that there is no expectation of privacy while using this system.

1.d.4 Separation of duties: ensure that administrative access for management of virtual servers is separated from administrative access for management of virtual networks. This is akin to the physical separation that is routine for system administrators and network operations personnel, respectively. Additionally, back-up administration should also be separated from both management of virtual servers and from management of virtual networks.

1.d.5 Management of hypervisors: management of hypervisors should be restricted to administrators only, and should be centralized. Local access for administrators to hypervisor management should not be authorized (i.e., console access should be used, and not a local user account).

1.d.6 Regularly make back-ups: just as with physical servers, virtual systems need to be regularly backed-up for error recovery. This includes recovering an entire server from a catastrophic event, and restoring individual files simply by mounting a back-up image. If possible, the data stream of a back-up should be encrypted to prevent the "theft" of a server image by capturing the packets in the backup.

> 1.d.6.1 Ensure that appropriate access control lists (ACLs) restrict copying or mounting images to authorized support personnel. If necessary, encrypt disk directories or partitions, as well as the back-up media itself.

1.d.7 Use separate back-up account: the backup process itself should use a dedicated backup account, with appropriate restrictions (no shell for instance). Under no circumstances should root be used for back-ups.

1.d.8 Follow disaster recovery (DR) procedures for virtual environment: ensure that DR planning takes the needs of hosts and VMs into account, as well as the physical infrastructure. While virtualization can be used as a recovery solution, the recovery of hosts and guests themselves must be planned for. That planning needs to include recovery time objectives for each VM running on each host (along with not mixing sensitivity levels on the same host). That is, each host should have VMs with the same recovery time objective and the same data sensitivity running on it.

1.d.9 Prevent “VM sprawl”: there is a tendency within organizations to allow the creation of more VMs than is necessary, for various reasons. This tendency can create a serious problem with the effective management of VMs. Require appropriate permission before VMs can be created, and before they can be deployed.

> 1.d.9.1 Creation and deployment of VMs should both be logged.

1.d.10 Control VM migration: effective management of VMs also requires controls around, and proper authorizations for the migration of VMs.

> 1.d.10.1 Migration of VMs should be logged (e.g., source and target systems, time, authorization).

1.d.11 Same risk level per host: all VMs on the same host should process the same level of data sensitivity, following an organization's data classification policy. For example, if designated for high sensitivity VMs, then all VMs on a designated host should be used for high sensitivity data only. Multiple levels of sensitivity should not be used on the same host.

1.d.12 Separate production from test VMs: production and test VMs should not run on the same host. Each host should be designated as either production or test, and run only appropriate (production or test) VMs.

1. Securing the virtualization platform

e. Logging and auditing

1.e.1 Use centralized logging: centralize logging of guest OSs, either on a separate logging system or in a repository. Use of centralized logging aids administrators, security personnel, and auditors in verifying configurations and practices in a virtualized environment (e.g., ensuring that configurations of guest OSs remain synchronized with regard to patches, updates and signatures).

1.e.2 Correlate logs: correlate server and network logs across virtual and physical infrastructures to reveal security vulnerabilities and risk. Use of a a security information and event management (SIEM) solution should at least be considered to aid in this recommendation.

1.e.3 Regularly audit virtualized environments: it is important to audit configurations of all components of a virtualized environment, management capabilities, virtual switches, virtual and physical firewalls, and other security devices (e.g., intrusion detection systems, anti-malware capabilities). Ensuring compliance with established configuration management practices is particularly important.

1.e.4 Root and administrative privileges: log and audit monthly root and administrative access and actions on all systems in a virtualized infrastructure.

1.e.5 Invalid logical access attempts: log and audit weekly all invalid logical access attempts on all systems in a virtualized infrastructure.

1.e.6 Access to all audit trails: log and audit monthly all access to audit trails on all systems in and supporting a virtualized infrastructure (e.g., a centralized log repository).

1.e.7 Initialization of audit logs: log and audit monthly initialization of all audit logs on all systems in and supporting a virtualized infrastructure (e.g., a centralized log repository).

1.e.8 Creation and deployment of VMs: log and audit monthly the creation and deployment of all VMs in a virtualized environment.

1.e.9 Migration of VMs: log and audit monthly the migration (e.g., source and target systems, time, authorization) of all VMs in a virtualized environment.

1.e.10 Creation and deletion of system-level objects: log and audit quarterly the creation and deletion of all system-level objects in a virtualized infrastructure.

1. Securing the virtualization platform

f. Platform network security

1.f.1 Restricted network access: network access for the host OS should be restricted to management services only, and, if necessary, network access to storage (iSCSI).

1.f.2 Use a firewall: a firewall should ideally be placed on the host OS to protect the system, or a firewall should at least be local to a small number of systems for protection purposes, with access allowed only for management purposes. Additionally, the firewall should restrict access to only those systems authorized to manage the virtual infrastructure.

1.f.3 Consider using introspection capabilities (e.g., firewalls, security appliances, and network IDS/IPS sensors) to monitor the security of the server and guest OSs. If the server or guest OS is compromised, its security controls may be disabled or reconfigured so as to suppress any signs of compromise. Having security services in the hypervisor permits security monitoring even when the server or guest OS is compromised.

1.f.4 Static IP addresses: ensure that host OS is assigned static and unique IP addresses.

1.f.5 Separate management network: management of host OS should be on a separate network than that used by guest OSs, using a separate NIC dedicated to management functions. Management network should be dedicated to management of the virtual infrastructure only, and *not* used for any other purpose – management of other systems or other uses.

1.f.6 Use encrypted communications: management of host OSs should only be done using encrypted communications, such as HTTPS, TLS, or SSH protocols, or encrypted virtual private networks (VPNs).

1.f.7 Restricted access through firewall: the firewall should by default deny all access on the management network to all systems and all ports other than those explicitly needed for authorized management of host systems, allowing only those services required and only with those authorized management IP addresses necessary.

1.f.8 Separate VLANs for host communications with guest OSs: host to guest OS communications should be on VLANs separate from guest-to-guest OS VLANs; to protect virtual switches, host-to-guest communications should not be commingled with guest-to-guest communications.

2. Securing virtualized workloads

a. Guest operating system hardening

2.a.1 Minimize number of accounts: guests should have accounts necessary for running each VM only with passwords that are strong, hard to guess, changed frequently, and only provided to staff that must have access. Separate credentials should be used for access to each guest OS; credentials should not shared across guest OSs, and should *not* be the same as used for access to the host OS.

2.a.2 Unnecessary programs and services: all unnecessary programs should be uninstalled, and all unnecessary services should be disabled. This action not only improves security, but will likely improve VM performance as well.

2.a.3 Configuration management: configuration management of guest OSs should be centralized to ensure that configurations are standardized. It is likely that multiple configurations will be required to meet business needs (e.g., high risk, medium risk, low risk, etc.), but deployed configurations must be documented in order to be effectively managed.

2.a.4 Patch management: guest OSs must be patched regularly and in a timely fashion to protect VMs. However, timeliness includes procedures for testing patches on non-production systems first to ensure that access to VMs is not disrupted.

2.a.5 Hardening guide: guest OSs should be hardened following an organization's approved hardening or build standard, which can be developed from independent guides (e.g., the Center for Internet Security, Defense Information Systems Agency, National Security Agency), or from vendor guidance.

2. Securing virtualized workloads

b. Virtual network security

2.b.1 Restricted network access: guest OS should not have management network access, but, if necessary, may have network access to storage (iSCSI).

2.b.2 Firewall: the guest OS should be protected by a firewall running on the host OS, or at least running locally (i.e., local to a small number of systems for protection purposes). Firewall needs to discriminate against inappropriate and/or malicious traffic using networking communications effective for the environment (e.g., if bridging is used instead of routing).

2.b.3 Consider using introspection capabilities to monitor the security of activity occurring between guest OSs. This is particularly important for communications that in a non-virtualized environment were carried over networks and monitored by network security controls (such as network firewalls, security appliances, and network IDS/IPS sensors).

2.b.4 Separate VLANs for guest OSs: each guest OS should run on a separate virtual local area network (VLAN) from other guest OSs that it does not need to communicate with. Assignment of separate VLAN IDs may require defining port groups for systems on the specific VLAN and allowing administrators to define different settings concerning network access and security policy for virtual machines connected to a single virtual switch. As many port groups as necessary may be created for a single virtual switch. Virtual network adapters associated with virtual machines may then be configured to connect to these user-defined port groups. The virtual adapters connected using a user-defined port group inherit and abide by the policies defined within the port group.

Appendix A – Glossary

- Full virtualization: a virtualization technique used to provide a virtual machine environment that is a complete simulation of the underlying hardware. In such an environment, any software capable of execution on the raw hardware can be run in the virtual machine and, in particular, any operating system.

- GRUB: short for GRand Unified Bootloader from the GNU Project. GRUB is a reference implementation of the Multiboot Specification, which enables a user to have multiple operating systems on their computer, and choose which one to run when the computer starts.

- Hypervisor (or virtual machine monitor, VMM): allows multiple operating systems to run concurrently on a host computer, a feature called hardware virtualization. The hypervisor presents the guest operating systems with a virtual platform and monitors the execution of the guest operating systems. In that way, multiple operating systems, including multiple instances of the same operating system, can share hardware resources. Unlike multitasking, which also allows applications to share hardware resources, the virtual machine approach using a hypervisor isolates failures in one operating system from other operating systems sharing the hardware.

- IDS: intrusion detection system is a network security device that tries to detect malicious activity such as denial of service attacks, port scans or even attempts to crack into computers by monitoring network traffic.

- IPS: intrusion prevention system is a network security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities.

- iSCSI: Internet Small Computer System Interface is an Internet Protocol (IP)-based storage networking standard for linking data storage facilities.

- Layer 2: Data Link Layer in the seven-layer OSI (Open System Interconnection) model of computer networking.

- NIC: network interface card is a computer hardware component designed to allow computers to communicate over a computer network.

- Paravirtualization: a virtualization technique that presents a software interface to virtual machines that is similar but not identical to that of the underlying hardware. The intent of the modified interface is to reduce the portion of the guest's execution time spent performing operations which are substantially more difficult to run in a virtual environment compared to a non-virtualized environment.

- SSH: Secure Shell is a network protocol that allows data to be exchanged using a secure channel between two networked devices.

- Type 1 (or native, bare-metal) virtualization: hypervisors run directly on the host's hardware to control the hardware and to monitor guest operating systems.

- Type 2 (or hosted) virtualization: hypervisors run within a conventional operating system environment. With the hypervisor layer as a distinct second software level, guest operating systems run at the third level above the hardware.

Appendix B – Sources

- Baldwin, Adrian, Simon Shiu, and Yolanta Beres, *Auditing in shared virtualized environments*, Trusted Systems Laboratory, HP Laboratories Palo Alto, HPL-2008-4, 2008.
- Butler, Michael and Rob Vandenbrink, *IT Audit for the Virtual Environment*, SANS, September 2009.
- Center for Internet Security, *Virtual Machine Security Guidelines Version 1.0,* September 2007.
- Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1*, December 2009.
- Foundstone, *How Virtualization Affects PCI DSS; Part 1: Mapping PCI Requirements and Virtualization*.
- Gulati, Rohit, *Security Best Practices for Hyper-V*, Microsoft TechNet.
- Hartman, Bret, Dr. Stephen Herrod, Charu Chaubal, and Nirav Mehta, *Security Compliance in a Virtual World*, RSA, The Security Division of EMC, August 2009.
- National Security Agency, *VMware ESX Server 3 Configuration Guide*, March 2008.
- U.S. Department of Commerce, National Institutes of Standards & Technology. *Recommended Security Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 3.
- U.S. Department of Defense, Defense Information Systems Agency. *ESX Server Checklist V1R1.4*, October 2009.
- VMware, *Achieving Compliance in a Virtualized Environment*, September 2008.
- VMware, *Network Segmentation in Virtualized Environments*, May 2009.