Cloud Computing Security

Rajendra Kachhwaha
rajendra1983@gmail.com

January 25, 2017

Outline

What is Guest OS Monitoring?

1. The hypervisor is fully aware of the current state of each guest OS it controls.
2. As such, the hypervisor may have the ability to monitor each guest OS as it is running, which is known as introspection.
3. Introspection can provide full auditing capabilities that may otherwise be unavailable.
4. Monitoring capabilities provided through introspection can include network traffic, memory, processes, and other elements of a guest OS.
5. For many virtualization products, the hypervisor can incorporate additional security controls or interface with external security controls and provide information to them that was gathered through introspection.
6. Examples include firewalling, intrusion detection, and access control.
7. Many products also allow the security policy being enforced through hypervisor-based security controls to be moved as a guest OS is migrated from one physical host to another.
8. Network traffic monitoring is particularly important when networking is being performed between two guest OSs on the host or between a guest OS and the host OS.

What is Guest OS Monitoring?

8. Network traffic monitoring is particularly important when networking is being performed between two guest OSs on the host or between a guest OS and the host OS.
9. Under typical network configurations, this traffic does not pass through network-based security controls, so host-based security controls should be used to monitor the traffic instead.

What is Image and Snapshot Management?

1. Creating guest machine images and snapshots does not affect the vulnerabilities within them, such as the vulnerabilities in the guest OSs, services, and applications.
2. However, images and snapshots do affect security in several ways, some positive and some negative, and they also affect IT operations.
3. Note that one of the biggest security issues with images and snapshots is that they contain sensitive data (such as passwords, personal data, and so on) just like a physical hard drive.
4. Because it is easier to move around an image or snapshot than a hard drive, it is more important to think about the security of the data in that image or snapshot.
5. Snapshots can be more risky than images because snapshots contain the contents of RAM memory at the time that the snapshot was taken, and this might include sensitive information that was not even stored on the drive itself.
6. An operating system and applications can be installed, configured, secured, and tested in a single image and that image then distributed to many hosts.

What is Image and Snapshot Management?

7. This can save considerable time, providing additional time for the contents of the image to be secured more effectively, and also improve the consistency and strength of security across hosts.
8. However, because images can be distributed and stored easily, they need to be carefully protected against unauthorized access, modification, and replacement. Some organizations need to have a small number of known-good images of guest OSs that differ, for example, based on the application software that is installed.
9. Image management can provide significant security and operational benefits to an organization. For example, if the contents of an image become compromised, corrupted, or otherwise damaged, the image can quickly be replaced with a known good image.
10. Also, snapshots can serve as backups, permitting the rapid recovery of information added to the guest OS since the original image was deployed.
11. One of the drawbacks associated with this type of backup is that incremental or differential backups of the system may not be feasible unless those backups are supported by the hypervisor.

What is Image and Snapshot Management?

12. If a modification is made to the guest OS after a snapshot has been captured, the original snapshot will not include the modification, and a new snapshot will need to be applied. Because of this, snapshot management needs to be considered as part of image management.
13. If an image has been compromised, its encapsulated nature means that it can easily be preserved for forensic purposes.
14. Also, a guest OS can be suspended quickly, which causes a snapshot to be recorded that captures the entire state of a compromised guest OS, including the complete contents of RAM, then stops the guest OS to prevent the compromise from spreading to other guest OSs or hosts.
15. In traditional environments, it is more difficult to capture the complete contents of RAM during or after an attack. Often, multiple steps must be performed before the data can be captured, potentially leading to the loss of important information.
16. Image files can be monitored to detect unauthorized changes to the image files; this can be done by calculating cryptographic checksums for each file as it is stored, then recalculating these checksums periodically and investigating the source of any discrepancies.

What is Hypervisor Security?

1. The programs that control the hypervisor should be secured using methods similar to those used to protect other software running on desktops and servers.
2. The security of the entire virtual infrastructure relies on the security of the virtualization management system that controls the hypervisor and allows the operator to start guest OSs, create new guest OS images, and perform other actions.
3. Because of the security implications of these actions, access to the virtualization management system should be restricted to authorized administrators only.
4. Some virtualization management systems allow different level of access to different users, such as giving some users read-only access to the administrative interface of a guest OS, other users control over particular guest OSs, and yet other users complete administrative control.
5. Most hypervisor software currently only uses passwords for access control; this may be too weak for some organizations security policies and may require the use of compensating controls, such as a separate authentication system used for restricting access to the host on which the virtualization management system is installed.

What is Hypervisor Security?

6. Hypervisors can be managed in different ways, with some hypervisors allowing management through multiple methods. It is important to secure each hypervisor management interface, both locally and remotely accessible.
7. The capability for remote administration can usually be enabled or disabled in the virtualization management system.
8. If remote administration is enabled in a hypervisor, access to all remote administration interfaces should be restricted by a firewall. Also, hypervisor management communications should be protected.
9. One option is to have a dedicated management network that is separate from all other networks and that can only be accessed by authorized administrators. Management communications carried on untrusted networks must be encrypted using FIPS-approved methods, provided by either the virtualization solution or a third-party solution, such as a virtual private network (VPN) that encapsulates the management traffic.
10. Because of the hypervisors level of access to and control over the guest OSs, limiting access to the hypervisor is critical to the security of the entire system. The access options vary based on hypervisor type.

What is Hypervisor Security?

11 Most bare metal hypervisors have access controls to the system. Typically, the access method is just username and password, but some bare metal hypervisors offer additional controls such as hardware token-based authentication to grant access to the hypervisors management interface.

12 On some systems, there are different levels of authorization, such as allowing some users to view logs but not be able to change any settings or interact directly with the guest OSs.

13 These view-only user accounts allow auditors and others to have sufficient access to meet their needs without reducing overall security.

14 In contrast to bare metal solutions, hosted virtualization products rarely have hypervisor access controls: anyone who can launch an application on the host OS can run the hypervisor.

15 The only access control is whether or not someone can log into the host OS. Because of this wide disparity in security, organizations should have security policies about which guest OSs can be run from bare metal hypervisors and which can be run from hosted virtualization hypervisors. Further, organizations running bare metal hypervisors should have policies specifying who can and cannot access various features of the hypervisor.

Security recommendations for the hypervisor

1. Install all updates to the hypervisor as they are released by the vendor. Most hypervisors have features that will check for updates automatically and install the updates when found. Centralized patch management solutions can also be used to administer updates.
2. Restrict administrative access to the management interfaces of the hypervisor. Protect all management communication channels using a dedicated management network or the management network communications is authenticated and encrypted using FIPS 140-2 validated cryptographic modules.
3. Synchronize the virtualized infrastructure to a trusted authoritative time server.
4. Disconnect unused physical hardware from the host system. For example, a removable disk drive might be occasionally used for backups, but it should be disconnected when not actively being used for backup or restores. Disconnect unused NICs from any network.
5. Disable all hypervisor services such as clipboard- or file-sharing between the guest OS and the host OS unless they are needed. Each of these services can provide a possible attack vector. File sharing can also be an attack vector on systems where more than one guest OS share the same folder

Security recommendations for the hypervisor

6. Consider using introspection capabilities to monitor the security of each guest OS. If a 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 guest OS is compromised.
7. 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 IDPS sensors).
8. Carefully monitor the hypervisor itself for signs of compromise. This includes using self-integrity monitoring capabilities that hypervisors may provide, as well as monitoring and analyzing hypervisor logs on an ongoing basis.

Perform a comparison of hypervisor securit in bare metal and hosted environment.

Read more from Paper : Characterizing Hypervisor Vulnerabilities in Cloud Computing Servers by Diego Perez-Botero, Jakub Szefer and Ruby B. Lee, ACM 2013.(Uploaded to GoogleClassroom)