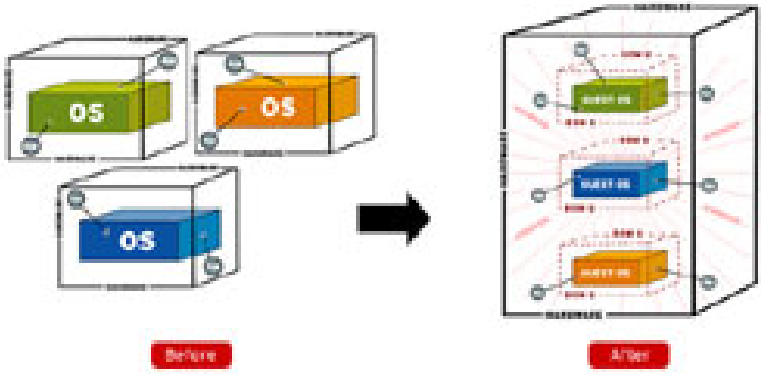
Security through virtualization

In this article, I will show you how to use security tools to increase the security of the Windows environment.

Deb Shinder



Network Administration - *We all know that virtualization can save companies a lot of money and simplify IT resource management, but whether it can be used to improve security. Confidential in systems and networks? From creating virtual honeypots and virtual honeynets to the use of Hyper-V to isolate server roles in order to seamlessly virtualize sandbox applications with the latest version of VMWare Workstation, the answer is completely may. This article will explore how you can use virtualization tools to increase the security of the Windows environment.*

Secure virtualization and virtualization for security

We've heard a lot about security issues that arise in virtualized environments, and most of them seem to focus on how to protect virtual machines (VMs). The truth is that virtualization technology can 'reveal' some security risks; however, when done properly, virtualization can also provide many security-related benefits.

Control is an important component in securing systems, including security within the organization and security of access to external network resources (eg external computers and servers). Mobile device used by remote users). Application virtualization gives you how to apply centralized control over applications that are accessed by multiple users, desktop virtualization that allows you to create isolated and secure environments to avoid applications. harmful websites or websites, .

Data concentration will make it easier for us to secure information, besides server virtualization technology allows sensitive data not to be stored on desktops or on laptops (easy storage) leads to data theft.

Sandbox

Sandbox is a quarantine environment used to secure applications that can harm the operating system or other applications and other networks safely. A virtual machine can directly access master resources, so it is more perfect for sandboxing. If you have an unsustainable application, have security or non-test vulnerabilities, then you can install it on a virtual machine so that if there is a security or compromise problem also does not affect the rest of the system.

Because web browsers are often a trail of dangerous software and attacks, effective security action is to run the browser in a virtual machine. You can also run other Internet-related programs - such as email clients, chat programs and P2P file sharing programs - in Vietnam. The VM has Internet access, but there is no access to the corporate LAN. This can protect the host operating system and enterprise programs, preventing access to internal resources from attacks on virtual machines via an Internet connection.

Another advantage is the ease of restoring virtual machines if it is compromised. The VM software provides backup of the machine images at specific times, which will simply restore the safe state before the deal takes place.

Virtual applications seamlessly and feel rich desktop with VMWare Workstation 6.5

The latest version VMWare Workstation (v6.5) provides the most integrated desktop experience with features that allow you to view individual applications from your home desktop virtual machine as if they were applications. running on the host operating system. For users, this makes integration of virtual applications much more seamless and thus increases satisfaction with the user's perception. You can drag and drop or copy and then paste between the virtual machine and the host that the user almost never knows the applications running in the virtual machines. That means that there are no longer complex factors related to sandboxing an application such as a web browser in a virtual machine.

The new software also allows you to set up a virtual machine that can be extended to multiple monitors. This is very useful when you need to run multiple applications side by side in a virtual machine. Or you can set up other virtual machines so that each virtual machine displays on a different screen, allowing you to easily check which virtual machine you are working at at some point. You can also run virtual machines in the background without using the Workstation user interface. You can find out more about VMWare Workstation 6.5's new features here.

Server isolation

Server consolidation is the main purpose for many businesses that use virtualization issues. Obviously, you can run multiple server roles on the same machine without virtualization; Your domain controller can also function as a DNS server, or a DHCP server, RRAS server, etc. However, having multiple roles on a server - especially a domain controller - will appear risky. tell about security. Virtualization will allow you to run all those roles on the same physical machine while still isolating the servers because they run on separate virtual machines.

Microsoft has designed Hyper-V to prevent unauthorized authentication between virtual machines. Each virtual machine runs in separate processes within parent partitions and runs with limited privileges in user mode. That helps protect the parent partition and hypervisor. Other security mechanisms have been equipped to isolate other virtual machines including distinguished virtualization devices, a distinguished VMBus from each VM to the parent partition, and no shared memory between VMs.

Note:
If virtual machine operating systems transmit content within them and share disks on a LAN, it will create a

vulnerability that can be exploited and negate some of the isolation effect in use. virtual machine.

Honeypot and Honeynet

Honeypot is a computer set up for the purpose of 'decoy' attackers, and honeynet makes an entire network consisting of honeypots. Honeynet seems like a production network. Its purpose is:

- To deflect attacks from your real production network
- Warn you in advance the types of attacks you have done so that you have time to protect against them on the network and 'real' systems.
- Logically collect information to be used to identify attacks

Honeypot and honeynet can be built using physical machines, but that can be expensive and difficult to manage. With virtualization technology, a large honeynet can be built on a physical machine at a much lower cost. Virtual desktops can surf the web to find out what viruses and malware are in which your AV software doesn't support protection.

Note:
As the best security operation, honeypots are equipped to deflect attacks from the Internet that need to run on a dedicated physical machine, which is not connected to your production network, or has firewalls set between them. Honeynet is typically placed in the perimeter or DMZ network. Another method is to place a honeypot on the internal network to detect the internal attacks.

Because so many organizations today run their consolidated servers on virtual machines, the virtual environment is perceived shortly before becoming a target for more interesting attackers for production networks. authentic.

Conclude

Properly deployed virtual machine technologies add another layer of security to the computers on your network. With the best security operations used, the operating systems and applications running on virtual machines will be secure and from there you will be able to safely protect them on physical machines. It is also the ultimate goal and that shows that virtualization is also one of the tools in your security arsenal.