PROSECURE™
SECURITY ARCHITECTURE BY NETGEAR®

Virtual Machines – Real Vulnerabilities

Where Virtualization Meets the Reality of Security

i7 Technologies Limited
Units 1-4
Hampton Heath Ind. Est.
Malpas
Cheshire
SY14 8LU

Tel: 01948 820787
Fax: 01948 820797

www.i7technologies.co.uk

Introduction

With the rapid adoption of virtualization over the past few years, an organization is more likely to have a virtual machine somewhere in its environment rather than not. According to IDC, virtualization growth rose year over year from 46% in 2007 to 54% in 2008. Virtualization offers many benefits including scalability, flexibility, rapid deployment of new servers, cost savings, and is energy efficient and thus environment friendly. With all these immediate benefits, it is no surprise that virtualization is quickly transforming the IT landscape.

With that said, what exactly is virtualization? Virtualization is the technology that allows the creation of virtual networking and computing resources on a single physical piece of hardware. These virtual resources all share the resources of a single physical host. This is all made possible by adding an additional hypervisor (also known as a virtual machine monitor) layer to the host server. The hypervisor allows multiple operating systems to concurrently run on the host computer.

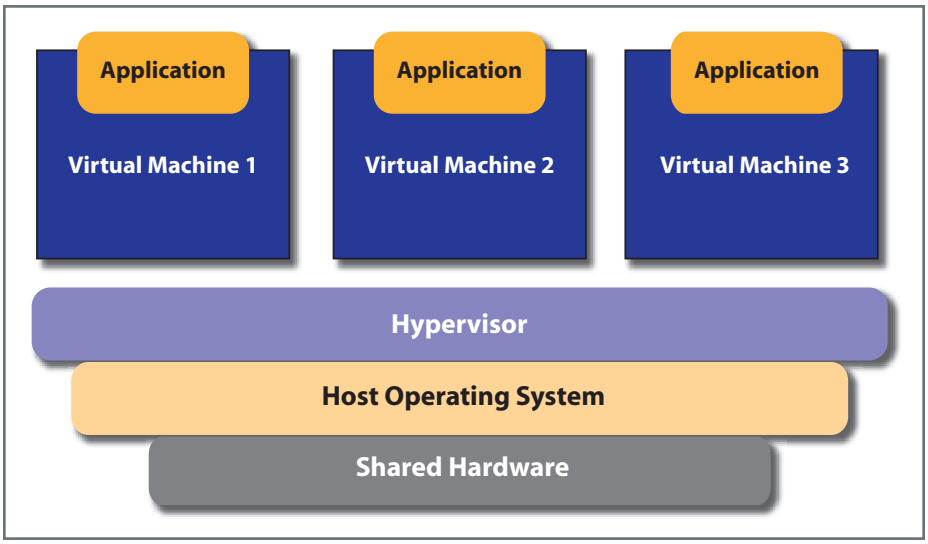

Figure 1. Virtualization Architecture

Hypervisor[1]

In computing, a hypervisor, also called virtual machine monitor (VMM), is a piece of software/hardware platform-virtualization software that allows multiple operating systems to run on a host computer concurrently.

There are two types of Hypervisors

Type 1 (or native, bare-metal) hypervisors are software the hardware control and to monitor guest operating-systems. A guest operating system thus runs on another level above the hypervisor.

Type 2 (or hosted) hypervisors are software applications running within a conventional operating-system environment. Considering the hypervisor layer as a distinct software layer, guest operating systems thus run at the third level above the hardware.

[1] Source: Wikipedia

Prior to virtualization, servers typically had a 1:1 software to hardware mapping. Meaning one operating system or application would run on one hardware server. For larger deployments this often meant hundreds to thousands of physical servers running in a data center environment. It takes substantial hardware, energy, deployment, and management costs to run such an environment. In addition to that, these servers were on average running at only 5% to 10% capacity, resulting in a huge waste of resources.

With virtualization organizations were able to run 10 or more virtual servers on a single host. What once was a 1:1 ratio now became 10:1 or even 20:1. It is not difficult to see the immediate and long term benefits virtualization brings.

Virtualization Security and Threats

With any new technology there will always be new threats and security concerns associated with it. Virtualization is no exception. In October 2007, Gartner's VP Neil MacDonald predicted that through 2009, 60 percent of production virtual machines (VMs) will be less secure than their physical counterparts. Below are some of the top security threats surrounding virtualization:

1. **Virtualization Specific Attacks** – Virtualization open up a new vector for potential attackers to exploit. There have been real world examples of compromised VMs being used to attack other VMs on the same host or even gain access to the host machine itself through the exploitation of memory space of devices shared by both the host and guest machines. Attacks on the hypervisor itself can potentially compromise all the VMs running above it.

2. **Traditional Threats** – Virtual machine exposure to threats are not limited to those targeted at VMs. Even with the physical aspect removed from them, VMs are still vulnerable to malware infection. Legacy viruses, Trojans, rookits, keyloggers, and other malware can all do substantial damage to a VM and its host. An infected VM can carry out attacks against other VMs as well as other physical servers on the network.

3. **Management Responsibilities** – Unlike physical servers where there is designated personnel to manage particular physical servers, the line with virtual machines is less clear. Oftentimes there are VMs that belong to multiple departments residing on the same host. Who manages the host? Who manages the individual VMs? Without a clear policy in place, the responsibility of managing and securing these VMs becomes a challenge and can lead to unattended VMs which can be exploited by attackers.

4. **VM Sprawl** – Virtual machines are so easy to create that it sometimes leads to VM sprawl. VM sprawl is the phenomenon of VMs increasing in an environment over time to the point where the infrastructure becomes less than optimal due to forgotten VMs with no real function taking away from the pool of shared resources. VMs, like traditional systems need to be properly patched and managed. Failure to do so can lead to huge security holes within the network.

5. **Virtual Machine Segmentation** – In traditional network environments critical servers are often located in their own dedicated VLANs, isolated from guest networks and the WAN. However the boundary between VMs is not as clear cut as the case with physical servers. A critical server can at times be deployed on the same physical host as a VM with far lower priority. Lower priority VMs have lower security requirements and have a higher chance of being compromised. From there attackers can potentially attack other guest VMs on the same hypervisor/host – essentially bypassing most of the security provided by the host machine.

Gateway Security in a Virtualized Environment

One aspect of the threats listed above which most organizations have more experience dealing with is traditional threats. This is a good starting point in securing your virtualized environment as many VM targeted threats still come in the network through traditional means such as spam and malformed Web pages. For years, servers and end user PCs have been attacked by a multitude of online threats. Millions of unique malware programs are created each year. Such malware is "pulled" onto user desktops through Web pages and spam emails. Because virtual machines are essentially "real" machines but with the physical aspect of them removed, they are just as vulnerable to these attacks as their physical counterparts. Most threats do not differentiate between virtual and physical machines. Spam will hit a mail server regardless of whether or not it is a VM. Virtual machines can get infected by executing virus code. Only this time, not only the VM itself is at risk, but also the hypervisor plus all the machines above it. Once the hypervisor itself is compromised, all is lost. All data and applications on the guest VMs are now at risk. All this time, the guest VMs are oblivious to the attack.

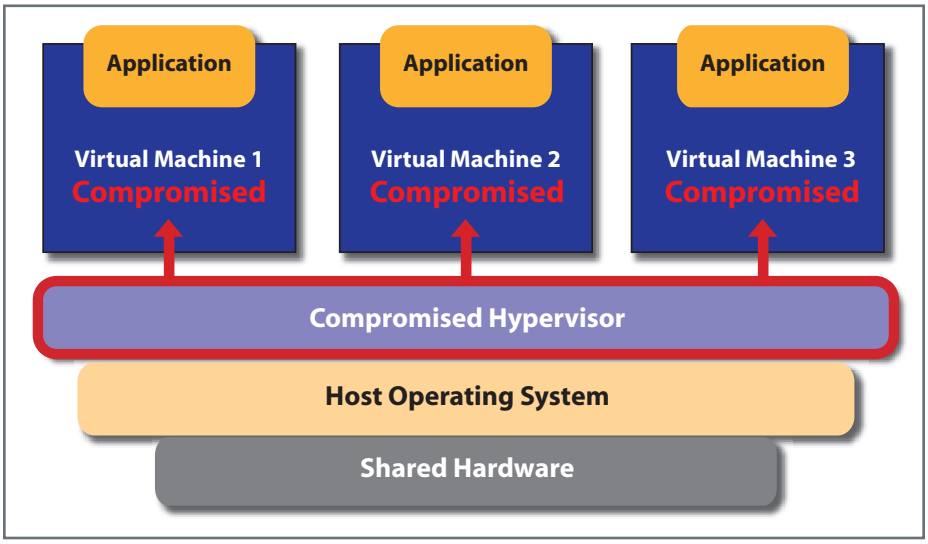

Figure 2. Compromised Hypervisor and VMs

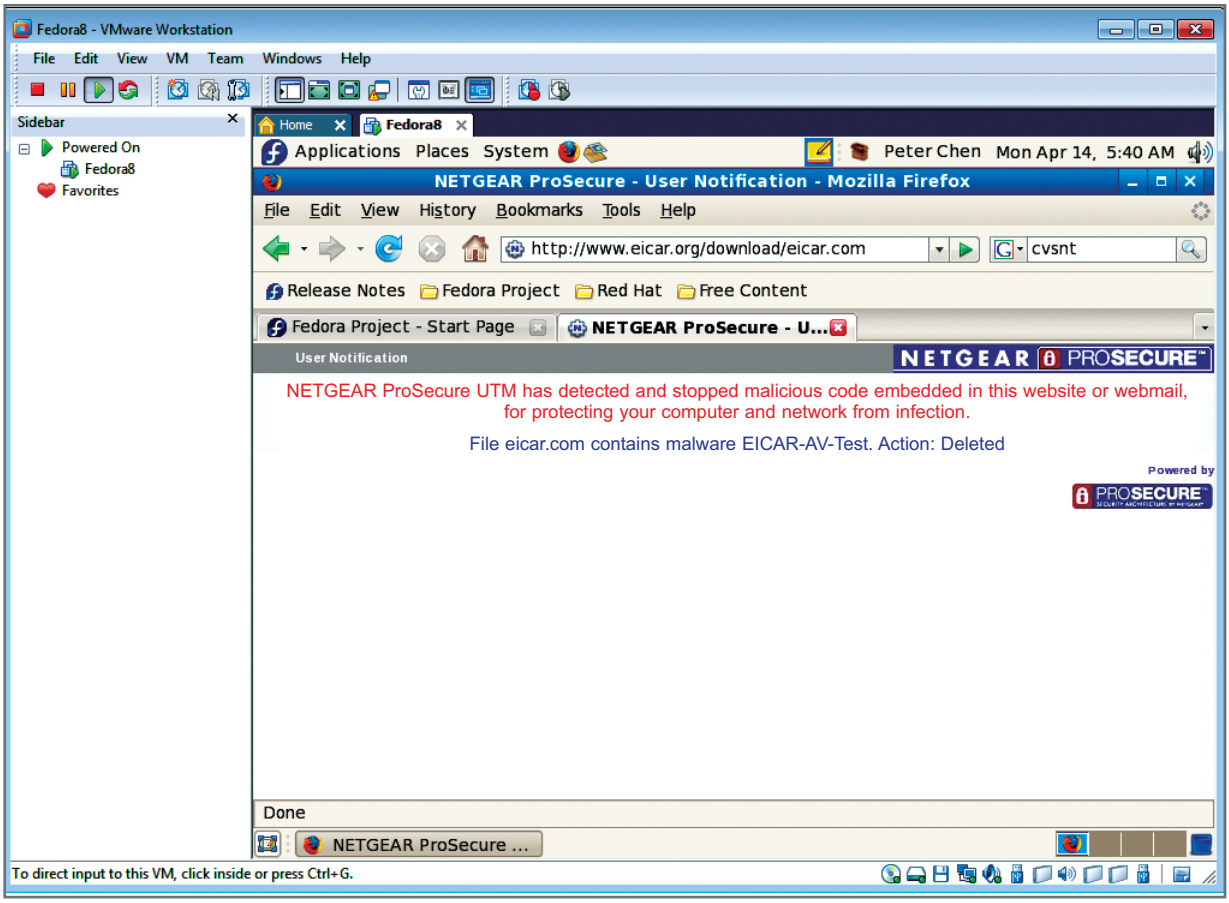

Figure 3. An attempt to download malware from a VM stopped by the ProSecure UTM

Traditional security measures and policies must be followed through more than ever. Anti-virus software must be deployed on each VM and especially on the host system itself. Access rights need to be clearly defined for each virtual resource. Optimally, a layered gateway security solution will be deployed at the network gateway. Intrusion prevention systems can thwart non-malware based attacks such as SQL injections. Anti-spam and Web filtering will prevent users from being exposed to malware carried through Web and email. For the malware that manages to bypass these layers, gateway anti-malware scanning should detect and remove the file before it reaches server or end user machines.

Figure 3 demonstrates the possibility of users pulling malware onto the VM. In this example the EICAR[2] test virus sample is stopped by the ProSecure gateway security appliance.

Conclusion

Virtualization has transformed the computing world. It represents the ability to rapidly deploy new servers, maximum usage of hardware resources, and a more streamlined computing environment. As more and more businesses rush to deploy virtual machines, they must also beware of the security issues specific to virtual environments. As a first step businesses should first secure their networks from general threats such as malware, spam, hacking, and unwanted Web content. A gateway security solution such as the ProSecure UTM mentioned in this paper will help simplify the deployment of gateway security by providing robust and effective layers of security on a single appliance.

ProSecure™ security appliances employ a best-of-breed security architecture that provides up to 400x the virus and malware coverage over other solutions at speeds up to 5x faster using patent-pending Stream Scanning technology.

***ProSecure™ STM Series**: For Medium Sized Businesses – Enterprise Strength Spam, Virus, & Web Filter Security*
***ProSecure™ UTM Series**: For Small Businesses – Comprehensive All-in-One Gateway Security – Without Compromise*

[2] The EICAR test file is a string of characters that will trigger most anti-virus engines. This file allows users to verify the functionality of their anti-virus engine without the use of real viruses. The file can be found at http://www.eicar.org/anti_virus_test_file.htm