Myths and Truths about Virtualization Security!

(Mythes et vérités de sécurité de virtualisation!)

John Reeman – CTO and Founder
Background

- Involved in IT Security for 18 years
- Contributing author to CIS (Center for Internet Security) ESX 3.5 Security benchmarks
- Developed VMinformer a unique security assessment monitoring tool for virtual environments
VirtSec Technology Landscape

• Today virtualization security is still an evolving technology space in terms of existing established security players as well as new startups & the virtualization platform vendors themselves.

• The next 12-18 months will be difficult for you the customer due to the gold rush effect.

• VMsafe was announced by VMware back in early 2008, vendor take up has been good but even today there are still only a handful of solutions that are commercially ready.

• There is (still) no silver bullet....
The Scoobydoo moment!

“what about security?”
Where do you start?

• The risks and threats
• Architecture and design
• Management
• Security controls
• Auditing and Monitoring
VMware Product Suite

- VMware vSphere 4
- VMotion
- Storage vMotion
- vShield Zones
- vCenter Server
- Lab Manager
- Life Cycle Manager
- Site Recovery Manager
- vOrchestrator

Larger Attack Surface
The potential threats

- Guest to Guest
- Host to Guest
- Guest to Host
- External to Host
- External to Guest
Don’t mix environments

No Security

Server VM's
Virus outbreak here

VDI VM's
effects Desktops here...

Firewall/IDP Appliance

Physical Switch
ogy merely enables you to consolidate servers by replacing physical servers with virtual servers that function exactly the same way — and need to be configured in much the same way — as their physical equivalents. You can consolidate servers in a DMZ using virtual technology and continue to rely on your existing security infrastructure.

Three Typical Virtualized DMZ Configurations

A virtualized DMZ network can fully support and enforce a wide range of configurations to separate trust zones. The three options described in this section are typical.

Partially Collapsed DMZ with Separate Physical Trust Zones

Organizations that want to keep DMZ zones physically separated tend to choose this method, shown in Figure 3. In this configuration, each zone uses separate ESX Server clusters. Zone isolation is achieved with physical security devices. The physical network does not require any change. The only difference between this configuration and a purely physical DMZ is that the servers within the trust zone are virtualized. This configuration limits the benefits you can achieve from virtualization because it does not maximize consolidation ratios, but this approach is a good way to introduce virtual technology into a network. Because it has minimal impact on an existing physical network, this configuration removes many risks. For instance, it minimizes the impact of the potential loss of separation of duties. This, in turn, greatly reduces the chance that an unqualified individual might be in a position to introduce a vulnerability through misconfiguration.

In this configuration, you do not need to configure dedicated virtual switches or use 802.1q VLANs within the virtual infrastructure. You perform all networking isolation on the physical network, not within the virtual infrastructure.

Advantages

- Simpler, less complex configuration
- Less change to physical environment
- Less change to separation of duties; less change in staff knowledge requirements
- Less chance for misconfiguration because of lower complexity

Disadvantages

- Lower consolidation and utilization of resources
- Higher costs because of need for more ESX hosts and additional cooling and power
- Incomplete utilization of the advantages of virtualization
vMotion

using a port scanner like nmap you can by simply scanning the vmotion port stop vmotion working!

vMotion Network should be isolated and if required encrypted using SSL
VM(in)Security Myth!

Security Team Says:

“Consolidating servers onto the same virtualized host is insecure because you cannot secure intra-VM traffic!”

Reality Check:

“When you have two physical servers plugged into the same physical switch in the same VLAN, how do you secure intra-machine traffic?”

Response:

Another Scoobydoo moment!
nifty Security options on vSwitches

- Protect against Forged Transmits - Enable
- Protect against MAC Address Spoofing - Enable
- Promiscuous mode - DISABLE
- By DEFAULT none of the above are set
Storage Layer

- Where is the data stored?
- How important is the data?
- Encryption?

“Isolate data according to environment”
Management

- VI Client - ESX or vCenter
- API’s - over 10+ currently available (VMCI Sockets)
- Web interface - ESX or vCenter
- Console (ESX)
Management - vCenter Security

Potential Risks
- Man in the middle attacks
- Brute force attacks
- sslniff
- SQL Injection

Good Design
- Isolate vCenter on a management network
- Change the default SSL Cert
- Lock down MSSQL
- Work on the principle of least privilege
Management - Protocols and Ports

- **HTTP**
  - 80
- **HTTPS**
  - 443
- **SSH**
  - 22
- **SMTP**
  - 25
- **SNMP**
  - 161
- **VNC**
  - 5900
- **NFS**
  - 2049
- **NTP**
  - 123
- **CIM**
  - 137
- **CIM (427)**
  - 3260

- **Can control using ESX Firewall**

- **Most TCP based some UDP**

- **2050-2250**
- **902,903**
- **5988**
- **5989**
- **8042-8045**

**Wednesday, February 10, 2010**
other considerations - Business Assets

- VM’s are business assets
- What function do they perform?
- Standard VMware management tools do not provide a business view
Security Controls

- Vendor provided - eg. VMsafe, vShield Zones
- Inbuilt Firewall on each ESX Host, IPTABLES
- 3rd Party Vendors, Firewall’s, IPS, Anti-Virus etc
- Configuration and lockdown
- Entitlement - Roles and Permissions
VMsafe Security API’s - quick overview

VMsafe Architecture – Closer Look

- **VMsafe-Net** - allows visibility of all I/O traffic on the host, inline protection or passive monitoring as well as ability to intercept, view, modify and replicate I/O traffic from one, many or all VM’s

- **VMsafe-Introspect (CPU-MEM)** - Inspection of specific memory pages being used by the VM or its applications, knowledge of CPU state, policy enforcement, little or no performance impact

- **VMsafe-Disk(VDDK)** - Ability to mount and read disks, inspect I/O read/writes to the storage device
VMsafe sample use cases

- **Verify-Before-Execute** - in-line memory based introspection of guest code execution
- **Virtual networks** - distributed and full-grain network monitoring stack for guest communication
- **File scanning** - scheduled scanning of offline and online VM’s.
- **Correlation** - multi-layered correlation engines in guest granularity
- **In-guest guarantees**: protecting in-guest components from in-guest malware
- **Early integrity checks** - early launch protection mechanisms for increased trust
Vulnerabilities - VMescape / VMbackdoor

• No known in the wild security vulnerabilities with the hypervisor yet

• There have been proof of concept VMescape exploit (Cloudburst) that target weaknesses in the virtual device drivers allowing guests to breakout and read data from the host or interact with other guests (has since been patched)

• This has happened with other virtualization platform vendors as well such as Citrix Xen server, blue pill, red pill, scooby etc
So what’s going on?

- Should you monitor?
- Do you monitor?
- VM Sprawl an issue?
- Policy Baselines?
Time for the Demo!!
VMinformer techie stuff

- Written in C# and .NET
- Policy files written in XML
- VM API Checks are user extensible
- SSH checks are closed except for file permissions
- DB Checks are user extensible
VMinformer Policies

- CIS Benchmarks
- ISO 27005
- DISA STIG
- My Own Research (undocumented key pairs)
Futures for VMInformer

• SIEM Integration
• Helpdesk Integration
• NMAP Support
• Deeper checks for VM Guests (VMsafe API)
• Scheduling
• Policy baselines
VMInformer

- Assess
- Identify
- Classify
- Context
- Report
- Remediate
Some Final thoughts....

• Remember there is no silver bullet

• Virtualization Security could end up costing you more if not planned well

• Design well, think about what you are trying to achieve or find someone who can help

• Thoroughly evaluate existing and emerging technologies to determine value vs disruption

• Use risk assessment and threat modeling

• VMware is NOT inherently INSECURE, its us damn humans that can mess it up!

• Monitoring and Auditing is IMPORTANT, don’t become complacent...

• Push the virtualization platform providers to reveal roadmaps, don’t always believe the hype!
Merci

communaute edition

disponible @

www.vminformer.com/community

john@vminformer.com