# VMware Security Best Practices

Chattanooga Information Security Professionals

# Stephen Haywood

I have been doing IT work for ten years and have focused on information security for the last five years. You can find me on the web:


Twitter – @averagesecguy

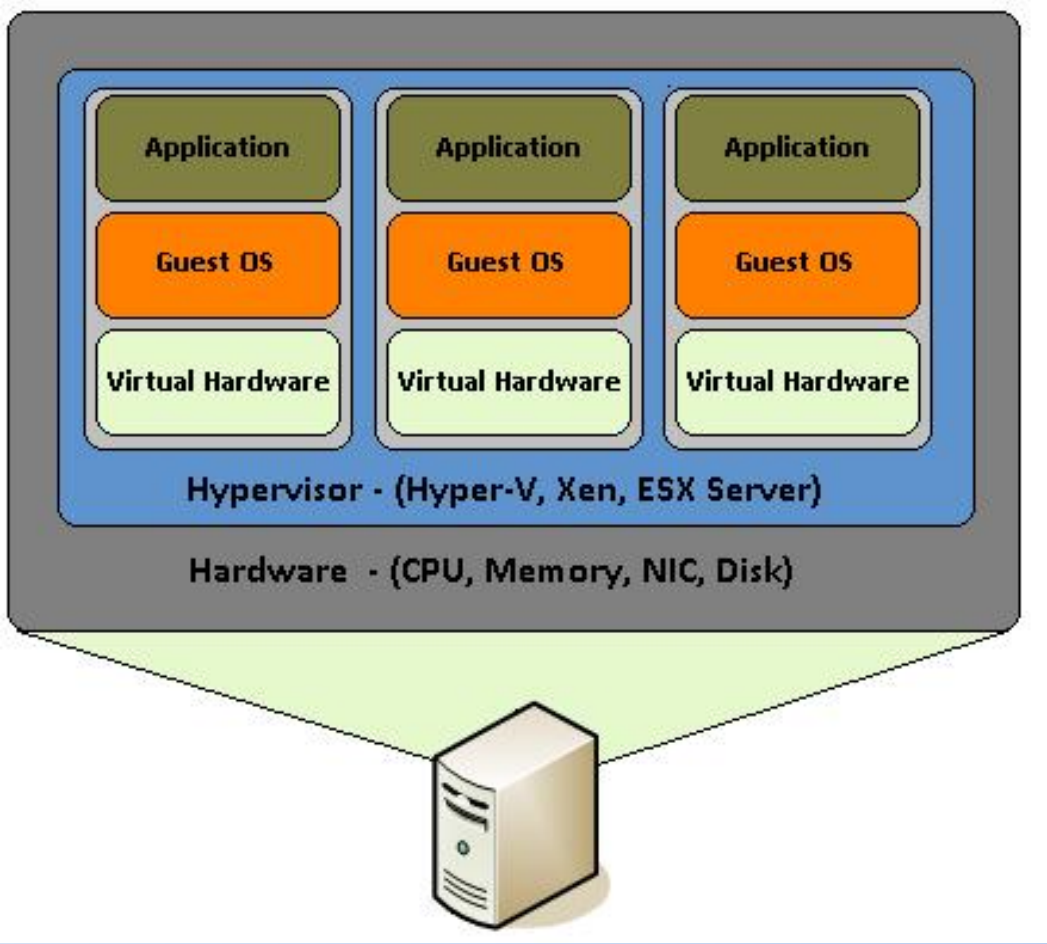
Blog – *averagesecurityguy.info*

Email – stephen@averagesecurityguy.info

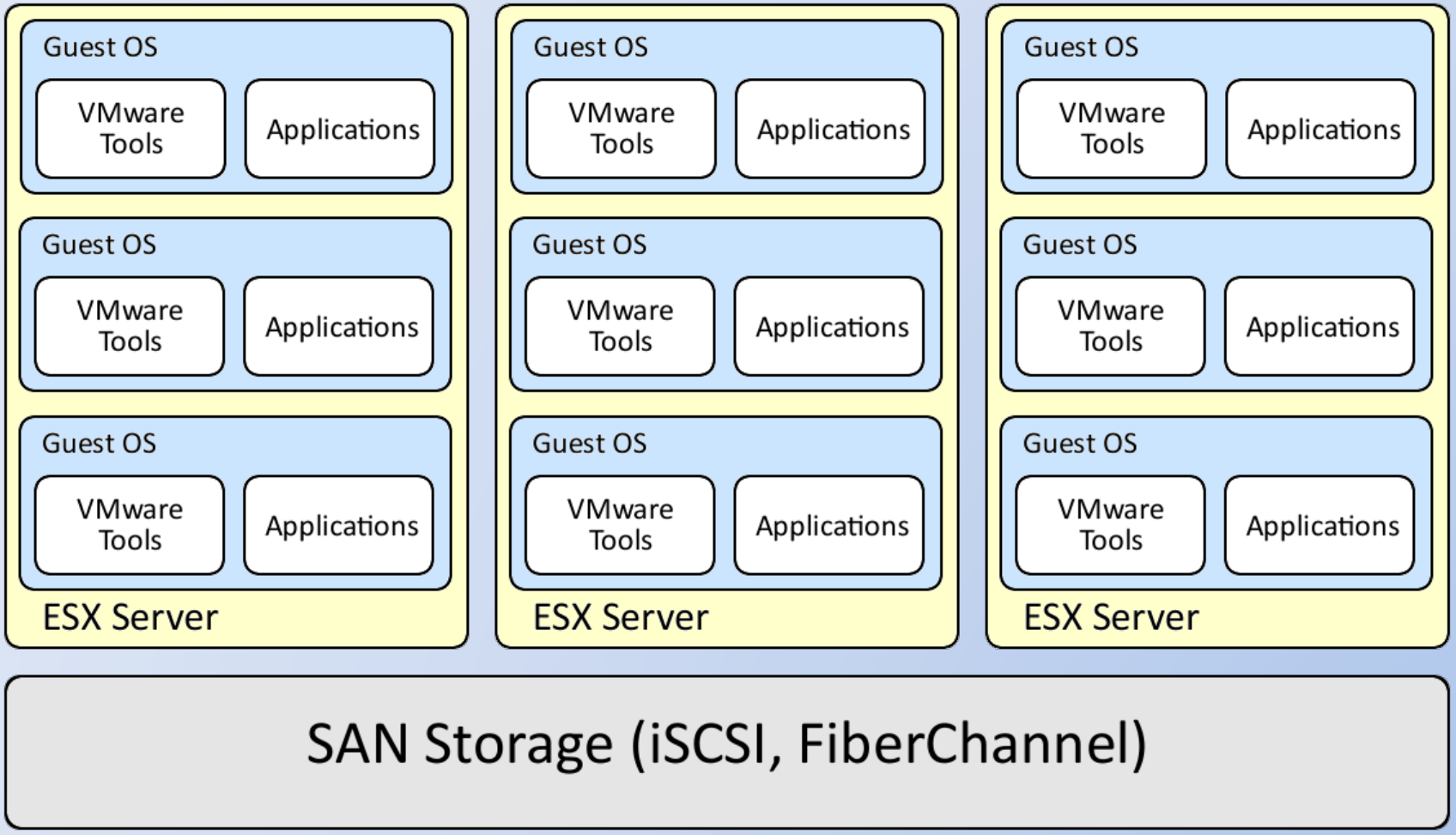
# The Basics

Virtualization is complex and there are many moving parts. We can't cover everything in this presentation. In other words, we will only cover the basics; the minimum things you should think about when installing or maintaining a VMware environment. Read the documents referenced in the handout for more details.

# What is Virtualization?



# VMware Environment



# Areas of Concern

- Storage System
- ESX Servers
- Guest Operating Systems

# Storage System

- Multiple Paths to Data
  - Each ESX server should have redundant HBAs not a single HBA with multiple ports
  - The SAN should have dual controllers
  - Should have dual switches (FC or iSCSI)
- iSCSI traffic should be a separate network
  - I like to see physical separation of traffic in different trust levels not VLANs.

# Storage System

- Share LUNs only with the appropriate HBAs
- Don’t share storage for systems in different security contexts
  - An external ESX server should not be using the same SAN as internal ESX servers.

# ESX Servers

- Server should be configured with redundant hardware including:
  - Power supplies, processors, NICs, HBAs
- Critical systems should have redundant ESX servers
  - If all your critical servers are on ESX then you need to load balance over multiple ESX servers (N + 1)

# ESX Servers

- Harden the ESX server
  - The *vSphere Hardening Guide* will tell you more than you want to know.
  - Recommendations are made on three trust levels: Enterprise, DMZ, and Specialized Security Limited Functionality

# ESX Servers

- Maintain security updates on the server
  - vCenter has a built in module that will scan your servers to identify missing updates and will install missing updates.
- Write logs to an external server
  - Write ESX server logs to a centralized logging system

# ESX Servers

- Don’t mix guests with different trust levels
  - You should not have DMZ virtual machines (VM) and internal VMs on the same ESX box. If an attacker compromises the DMZ VM they may be able to access the internal network using a VM escape.
- Disable Web access to the ESX server and use the vCenter client or Web access instead
- Control physical access to the ESX servers

# Guest Operating Systems

- Harden the Guest OS
  - Each guest OS should be hardened to match the security context in which it resides.
  - Use templates to deploy VMs.
- Apply security updates to the Guest OS and third-party applications
  - Just like a physical machine you have to maintain security updates for the OS and any third-party applications.

# Guest Operating Systems

- Keep VMware tools updated
  - Update the VMware tools as necessary.
- Be careful of dormant VMs
  - May have an unused VM that is shutdown for six months or a year and then it is brought back online.

# Guest Operating Systems

- Backup your VMs.
  - Redundant storage and replication does not take the place of backups.
- VMs are just files and need to be secured appropriately

# Say What?