FANSHAWE

INFO-6003

O/S & Application Security

Week 10

Agenda

- Types of Virtualization
- Host Based Virtualization
- Hypervisor Based Virtualization

Test 02

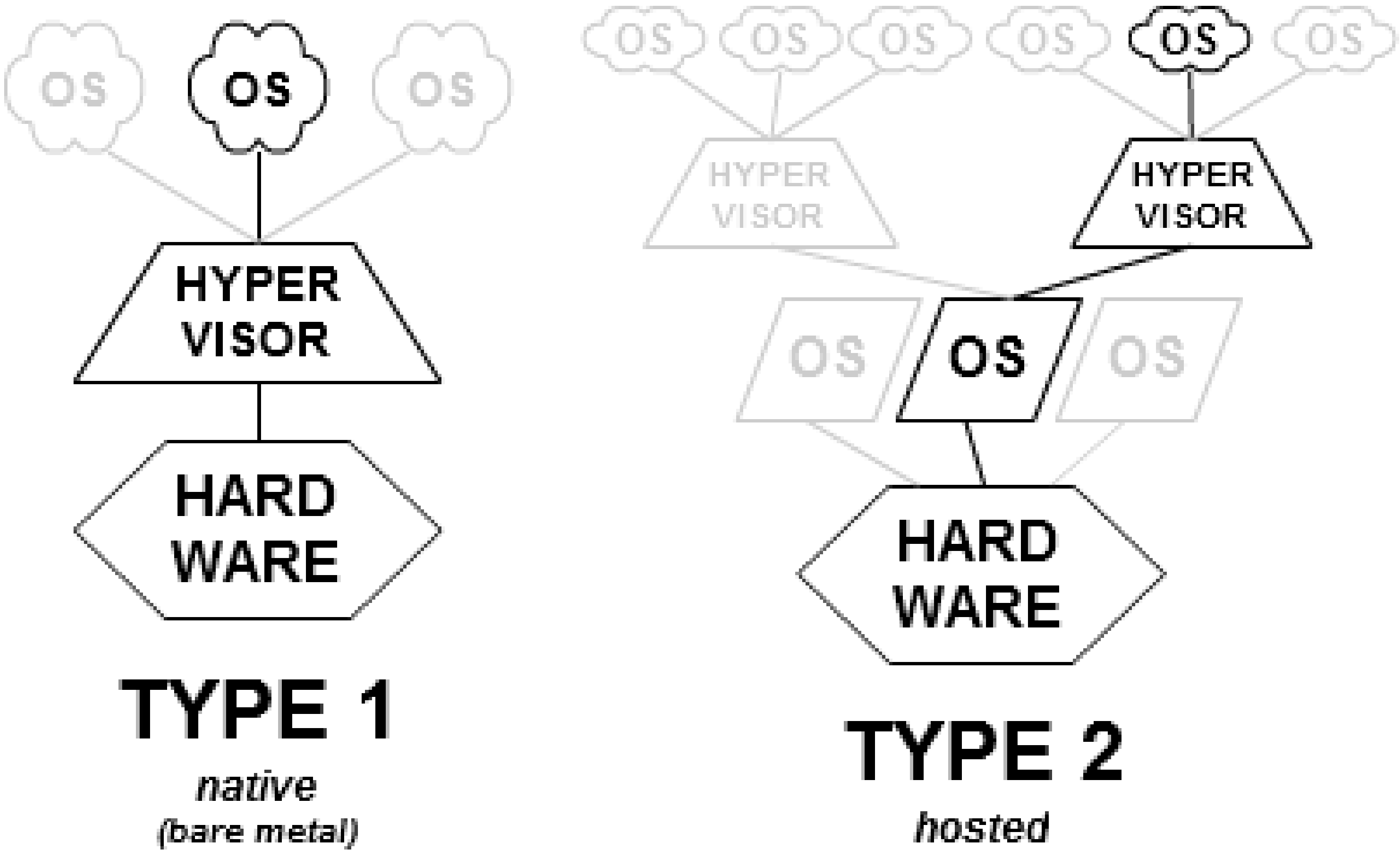
- Reminder for Test-02
- When: Next week
- Where: Regular Room
- Time: Regular Time

Virtualization

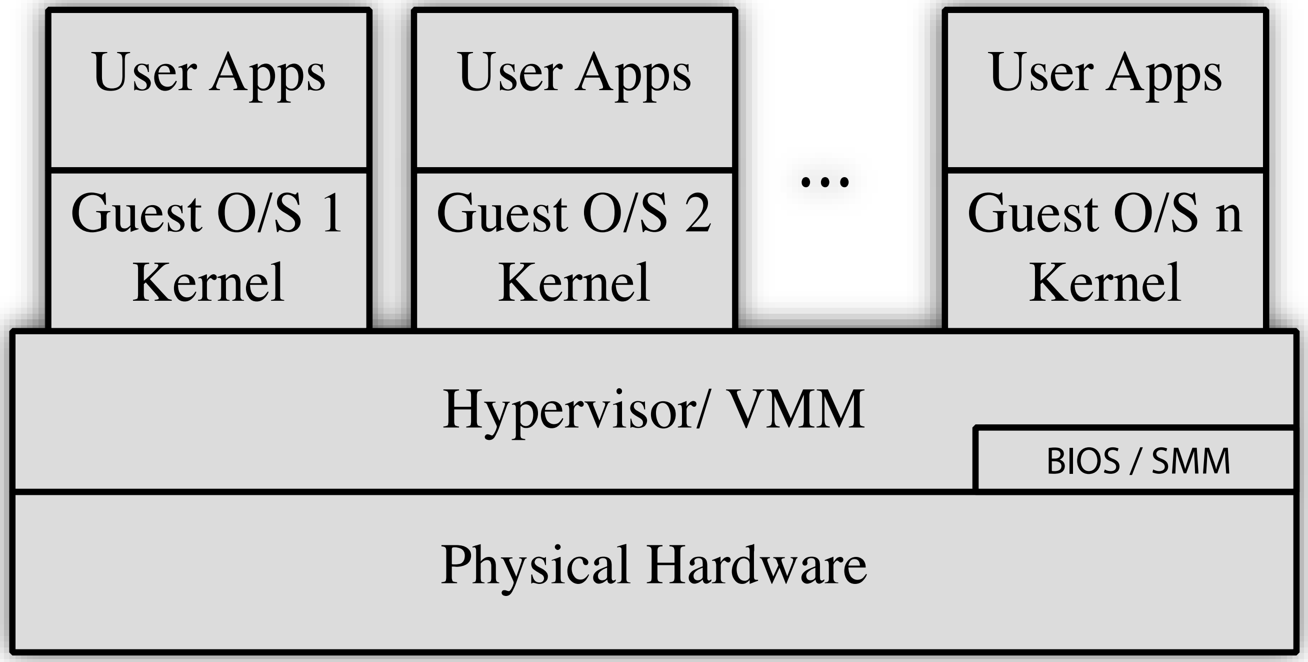
Types of Virtualization

- Type1
  - Also known as a Bare Metal Hypervisor
  - The hypervisor is installed directly onto the hardware
  - The hypervisor has more direct access to the hardware
    - More Efficient, but More Expensive
- Type 2
  - Referred to as Hosted, Host based, or OS based
  - The hypervisor is running on top of another operating system: Windows, Linux, OSX
  - The OS is sitting between the hypervisor and the hardware
    - Less Efficient, but Less Expensive

Type 1 vs Type 2

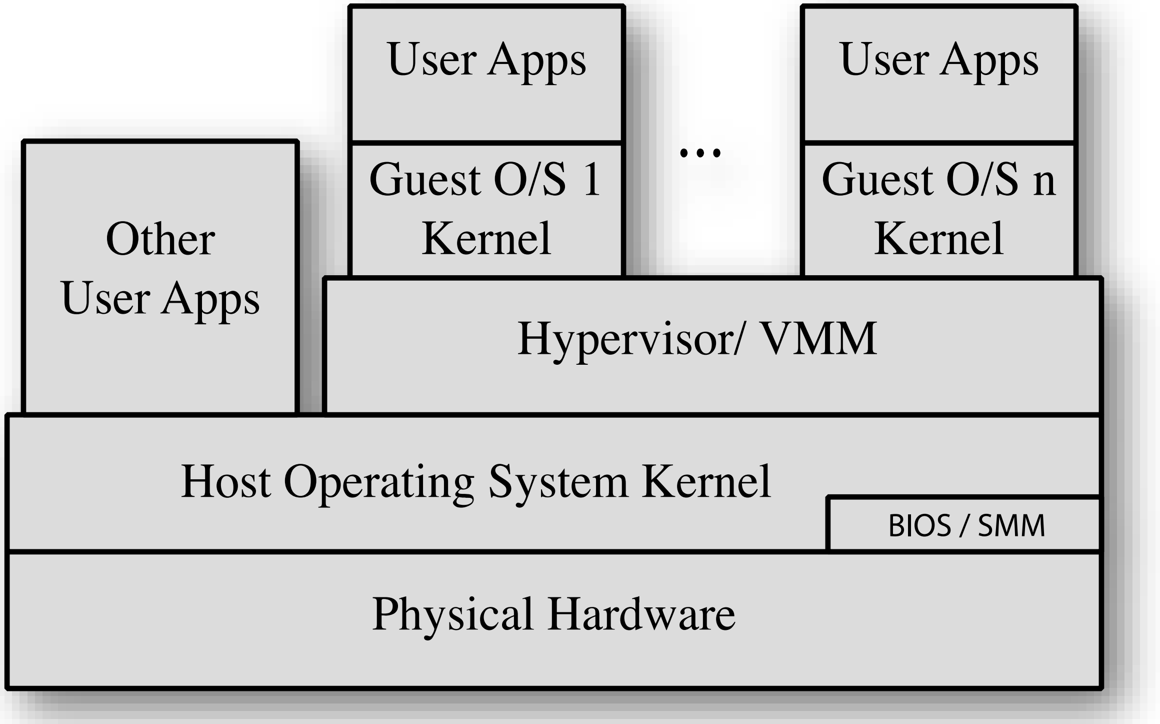


Type 1 - Bare-Metal Hypervisor



- A Bare-Metal Hypervisor system does not require another operating system

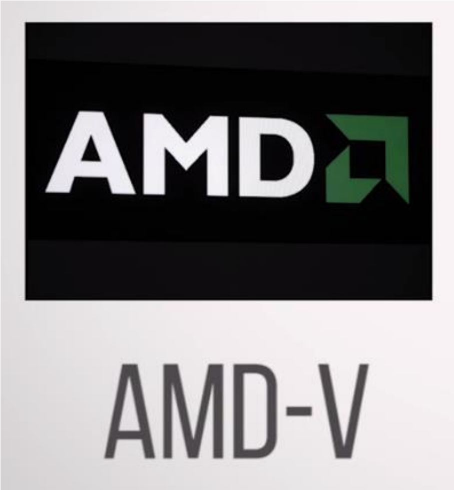
Type 2 - Host-Based Virtualization



- Host OS
  - Windows, Linux, OSX
- Hypervisor
  - VMware Workstation, VMware Fusion

Hypervisor Support by CPU

- Both Intel and AMD made progress in natively supporting virtualization on their chips in the mid 2000’s
- Ensure that this feature is enabled in your BIOS settings



VMWare Workstation Terminology

Host – The physical computer you install VMware Workstation on is called the host computer, and its operating system is the host operating system.

Guest – The operating system running inside a virtual machine is called the guest operating system.

Host-Based Virtualization

- Has a variety of Uses
  - Desktop Replacement
  - Development and Testing
    - Especially useful in a security context
  - Sharing VMs with other team members
  - Multi-OS Environments
    - Helpful when you are supporting more than one OS

VMWare Tools

- There is a lot of Host to Guest OS integration available when you are using Workstation
  - Copy/Paste
  - Drag/Drop
  - Shared Folders from the Host Machine
- VMware tools must be installed to use these features
- Every version of Workstation comes with a specific version of VMware Tools
- To ensure your VMs work properly you need to make sure you are using the correct version of VMware Workstation and Tools

Transferring Files

- These features increase functionality, but reduces the overall security by reducing the amount of VM isolation
  - – Copy/Paste
  - – Drag/Drop
  - – Shared Folders from the Host Machine

- VMware tools must be installed to use these
    - VM – Settings – Options – Guest Isolation

Preserving VM States

- There are a variety of ways to preserve your guest operating system's state, providing you with a recovery path
- Snapshots
  - Taking an image of the VM at a specific point in time
    - After_Lab-01, After_Lab-02, etc.
- Suspend / Resume
  - Kind of like pause and play
- Cloning
  - Creating an entirely new VM

Suspend / Resume

- There are two ways to suspend a VM
  - Soft = “Suspend Guest”
    - This suspends the VM and releases the IP address
  - Hard = “Suspend”
    - The VM is simply stopped
- These settings can be modified under
  - VM – Settings – Options – Power

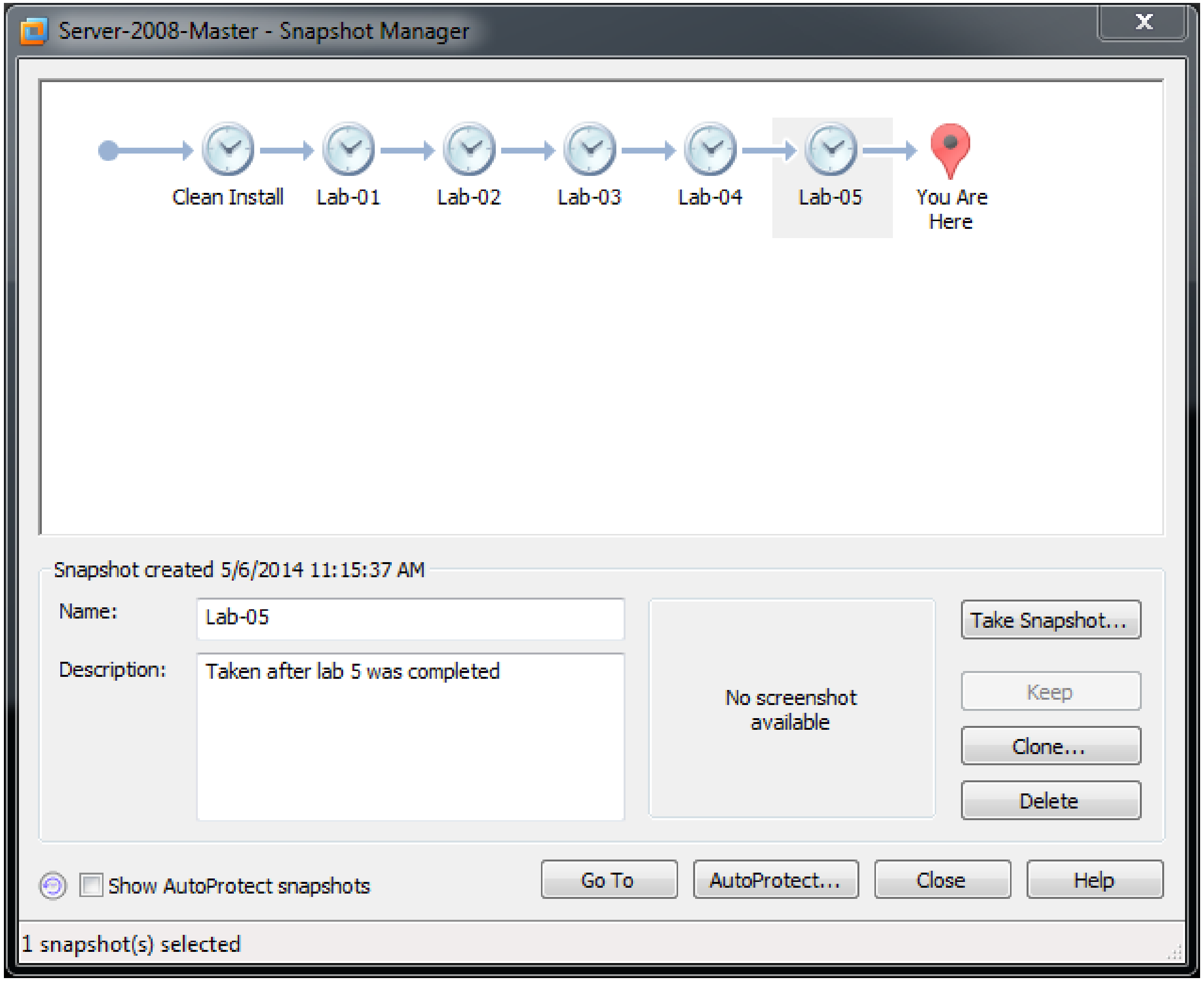
Snapshots

- Snapshots preserve the VM state so that you can return to the same state repeatedly
  - Very useful when testing the effects of malware and viruses
  - Can also be useful if you want to do a lab again when you are studying
- Information captured in a snapshot
  - Memory State: Contents of the virtual machine memory
  - Settings State: Virtual machine settings
  - Disk State: State of all the virtual disks

Types of Snapshots

- Snapshots are taken in two ways:
- Linear
  - Take a snapshot and continue to use the VM from that point
  - Can restore to any point along the line
  - Supports over 100 snapshots
- Process Tree
  - Multiple Nested snapshots
  - Supports over 100 snapshots per branch
  - This is the model used when you are using snapshots to do your labs again when studying

Linear Snapshots



Snapshot created 5/6/2014 11:15:37 AM

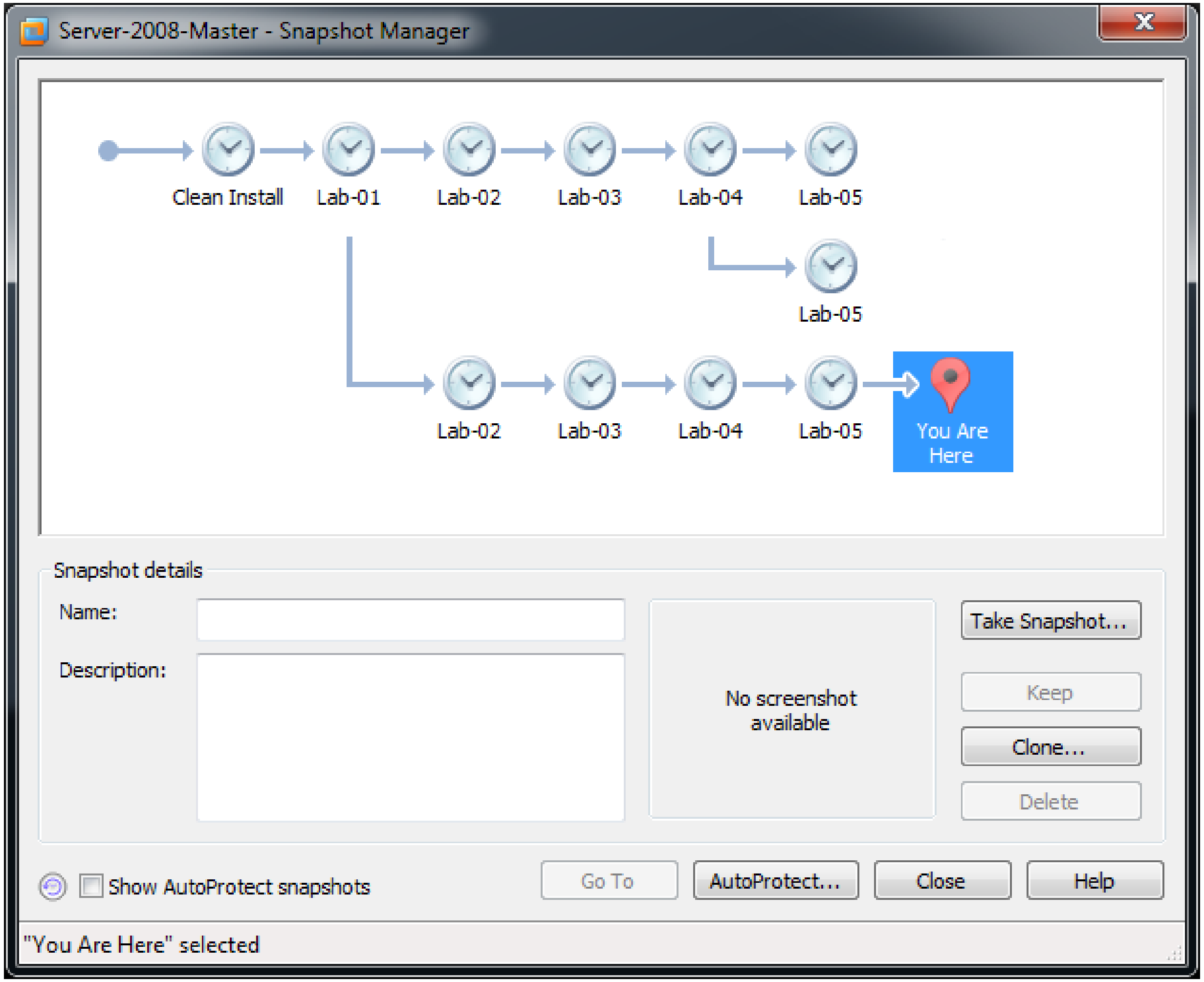
Name: Lab-05

Description: Taken after lab 5 was completed

No screenshot available

1 snapshot(s) selected

Process Tree Snapshots



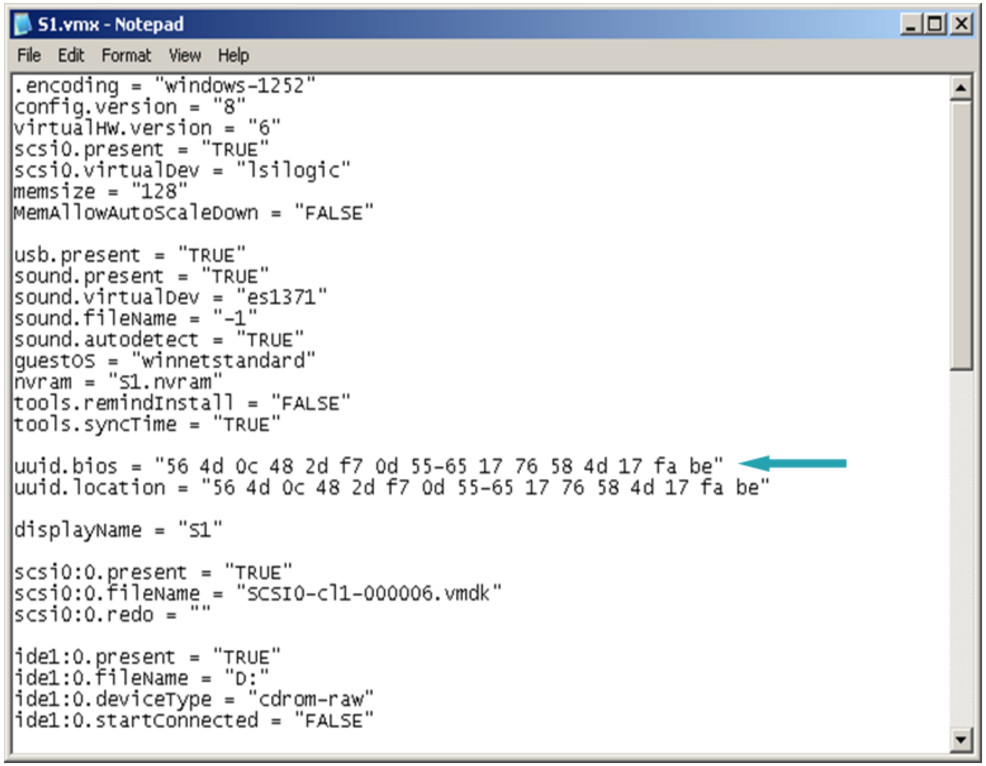
"You Are Here" selected

Cloning

- Full Clones
  - Self contained copy of original VM
- Linked Clones
  - Copy of original VM
    - Requires the original VM to be accessible
    - If you delete the original, the linked clone will be inaccessible
- UUID
  - Universally Unique Identifier
  - Unique ID of each VM and its location

UUID Location

- vmx Vmware Configuration File
- 128 bit - Unique for each VM



```
.encoding = "windows-1252"
config.version = "8"
virtualHW.version = "6"
scsi0.present = "TRUE"
scsi0.virtualDev = "lsilogic"
memsize = "128"
MemAllowAutoScaleDown = "FALSE"

usb.present = "TRUE"
sound.present = "TRUE"
sound.virtualDev = "es1371"
sound.fileName = "-1"
sound.autodetect = "TRUE"
guestOS = "winnetstandard"
nvram = "S1.nvram"
tools.remindInstall = "FALSE"
tools.syncTime = "TRUE"

uuid.bios = "56 4d 0c 48 2d f7 0d 55-65 17 76 58 4d 17 fa be"
uuid.location = "56 4d 0c 48 2d f7 0d 55-65 17 76 58 4d 17 fa be"

displayName = "S1"

scsi0:0.present = "TRUE"
scsi0:0.fileName = "SCSI0-cl1-000006.vmdk"
scsi0:0.redo = ""

ide1:0.present = "TRUE"
ide1:0.fileName = "D:"
ide1:0.deviceType = "cdrom-raw"
ide1:0.startConnected = "FALSE"
```

UUIDs

- uuid.bios
  - identifies the virtual machine hardware
- uuid.location
  - identifies the location of the virtual machine
  - if you move the VM you will be asked if you moved or copied the VM
  - if you copied it, you will want to create a new UUID to prevent conflicts with the existing VM

Full Clones

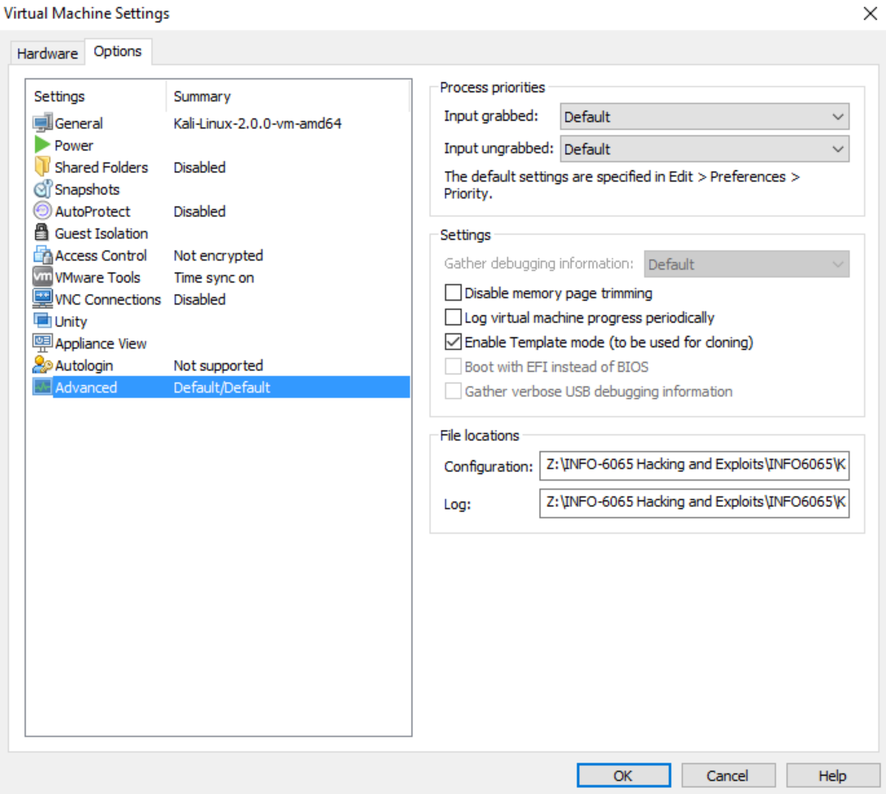
- Same settings as original
    - Changes to clone or parent don’t affect the other
- MAC and UUID are changed when cloned
- Clones can only be created when VM’s are powered off
- Another way to create a clone is to simply copy the files
    - – Can cause problems with conflicting UUIDs because VMWare doesn’t create new ones

Linked Clones

- Shares parent Virtual disk on an ongoing basis
  - Must have access to the parent
- All files available on the parent at the moment you take the snapshot continue to remain available to the linked clone
  - Ongoing changes to the virtual disk of the parent do not affect the linked clone
  - Changes to the disk of the linked clone do not affect the parent
- Slower to start, but conserve disk space

Linked Clones

- Template mode
  - Locks the parent so that it can’t be deleted
  - VM – Settings – Options – Advanced



Virtual Machine Settings

Settings	Summary
General	Kali-Linux-2.0.0-vm-amd64
Power	
Shared Folders	Disabled
Snapshots	
AutoProtect	Disabled
Guest Isolation	
Access Control	Not encrypted
VMware Tools	Time sync on
VNC Connections	Disabled
Unity	
Appliance View	
Autologin	Not supported
Advanced	Default/Default

Process priorities

Input grabbed: Default

Input ungrabbed: Default

The default settings are specified in Edit > Preferences > Priority.

Settings

Gather debugging information: Default

□ Disable memory page trimming

□ Log virtual machine progress periodically

☑ Enable Template mode (to be used for cloning)

□ Boot with EFI instead of BIOS

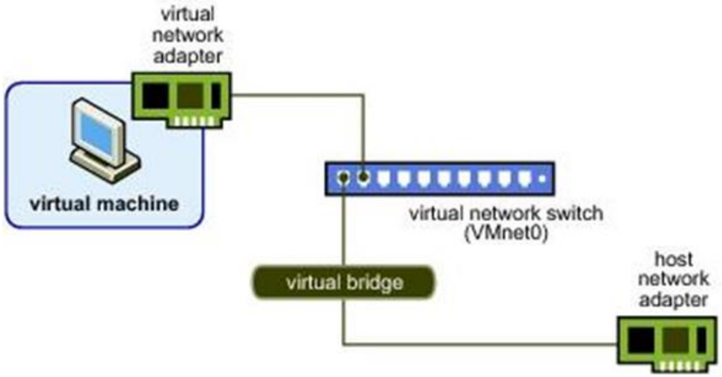
□ Gather verbose USB debugging information

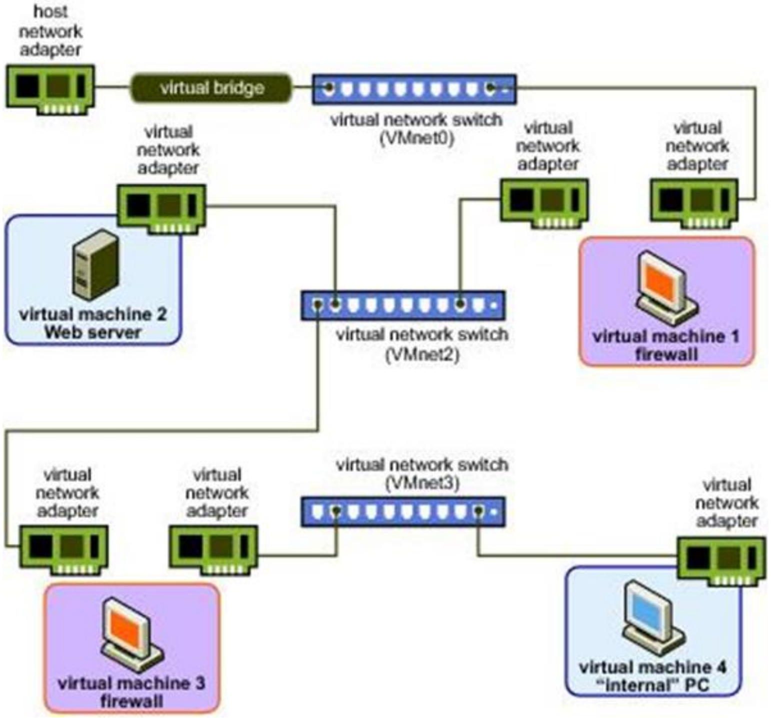
File locations

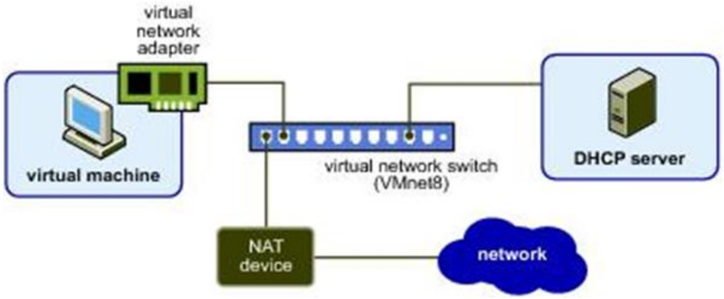
Configuration: Z:\INFO-6065 Hacking and Exploits\INFO6065\K

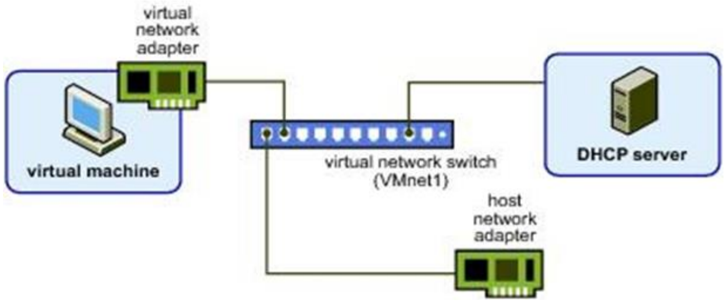
Log: Z:\INFO-6065 Hacking and Exploits\INFO6065\K

Virtual Network Switches

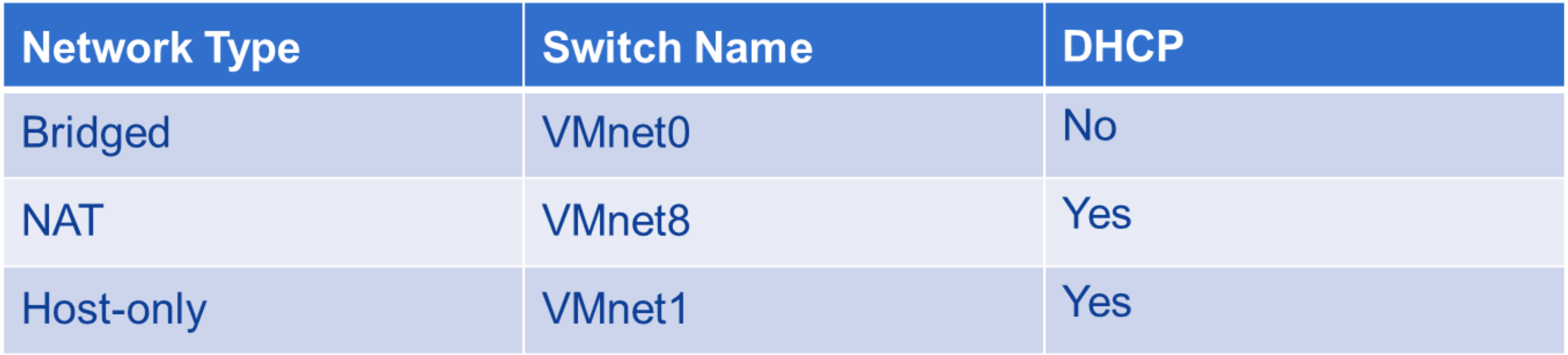



host network adapter
virtual bridge
virtual network switch (VMnet0)
virtual network adapter
virtual network adapter
virtual network adapter
virtual machine 2 Web server
virtual network switch (VMnet2)
virtual machine 1 firewall
virtual network adapter
virtual network adapter
virtual network switch (VMnet3)
virtual network adapter
virtual machine 3 firewall
virtual machine 4 "internal" PC





Virtual Switches

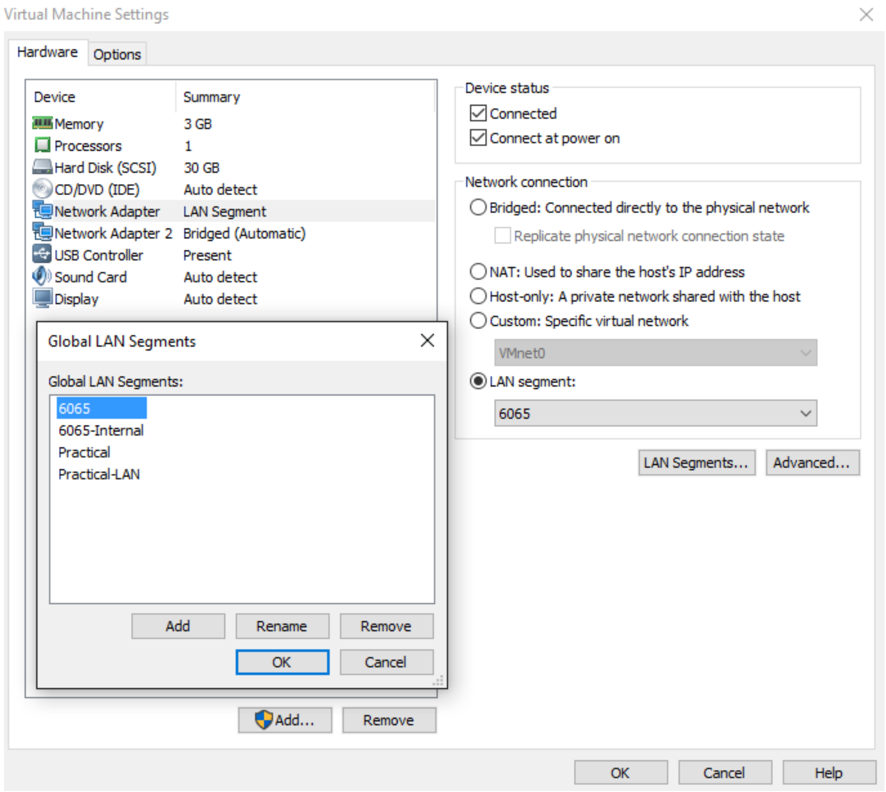


Network Type	Switch Name	DHCP
Bridged	VMnet0	No
NAT	VMnet8	Yes
Host-only	VMnet1	Yes

- Can be viewed through the Virtual Network Editor
- Maximums:
  - 10 virtual switches on Windows
  - 255 virtual switches on Linux

NIC: LAN Segments

- Provides complete isolation of VMs from host
- Inaccessible/Undetectable from other networks
- Very good for testing environments



Virtual Machine Settings

Hardware | Options

Device	Summary
Memory	3 GB
Processors	1
Hard Disk (SCSI)	30 GB
CD/DVD (IDE)	Auto detect
Network Adapter	LAN Segment
Network Adapter 2	Bridged (Automatic)
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Device status

☑ Connected

☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network

□ Replicate physical network connection state

○ NAT: Used to share the host's IP address

○ Host-only: A private network shared with the host

○ Custom: Specific virtual network

VMnet0

● LAN segment:

6065

Global LAN Segments

Global LAN Segments:

6065

6065-Internal

Practical

Practical-LAN

Network Types

- Bridged
  - Connected to your laptops physical NIC
  - No isolation
  - VMware doesn’t provide DHCP
- Host Only
  - Connected to virtual NIC on laptop
  - Isolated from the Internet
  - VMware provides DHCP
  - VMs on network can talk to each other and host computer

Network Types

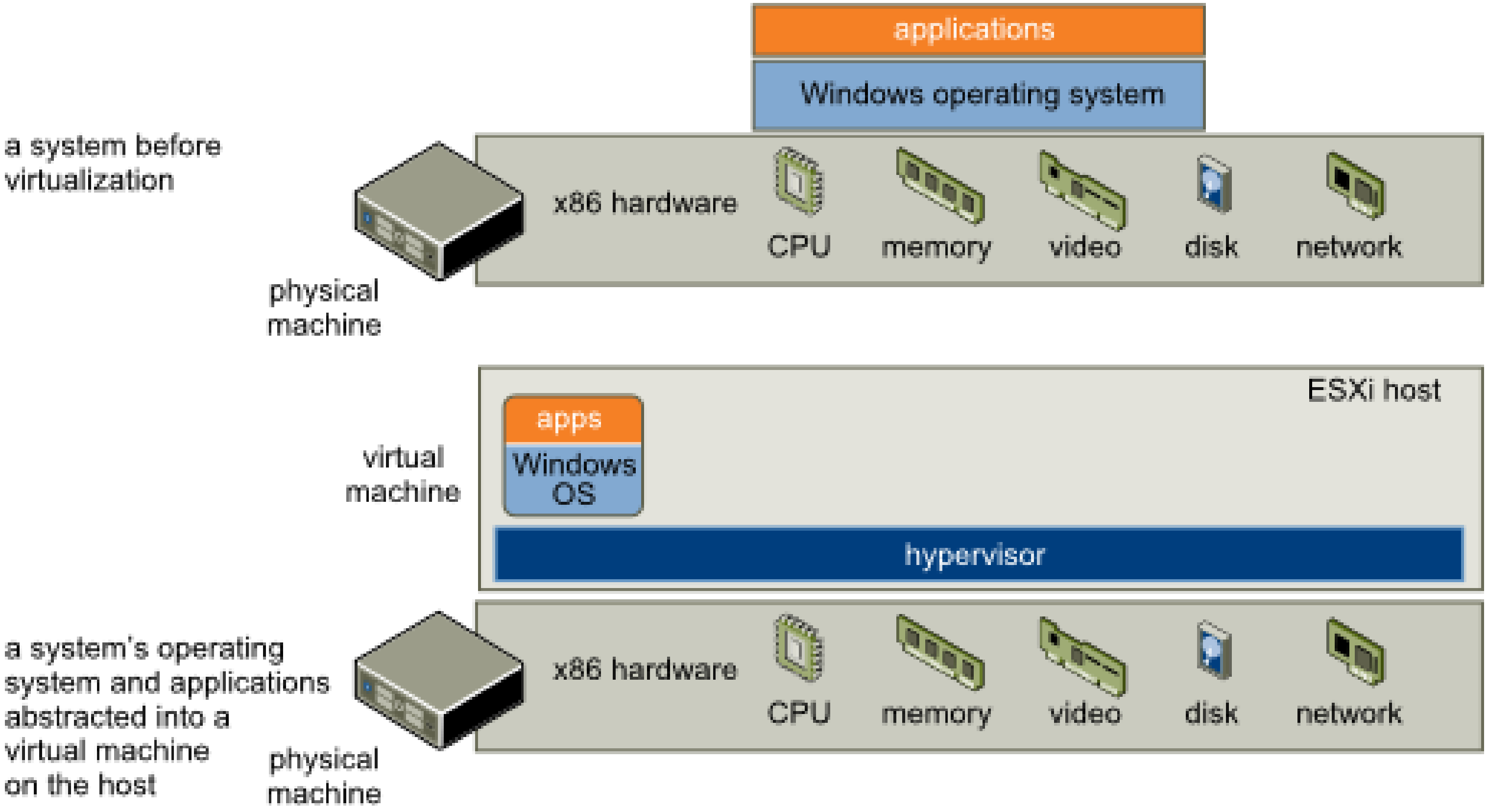
- NAT
  - Connected to virtual NIC on laptop
  - Not isolated from the Internet
  - VMware provides DHCP
  - VMs on network can talk to each other, host computer and the Internet

Virtual Network Details

- Custom vmnet (most similar to host-only)
  - Connected to virtual NIC on laptop
    - Created when you create the custom vmnet
  - Isolated from the Internet
  - VMware provides DHCP
  - VMs on network can talk to each other and host computer
- LAN Segment
  - No virtual NIC on laptop
  - Completed isolated from laptop
  - VMware doesn’t provide DHCP

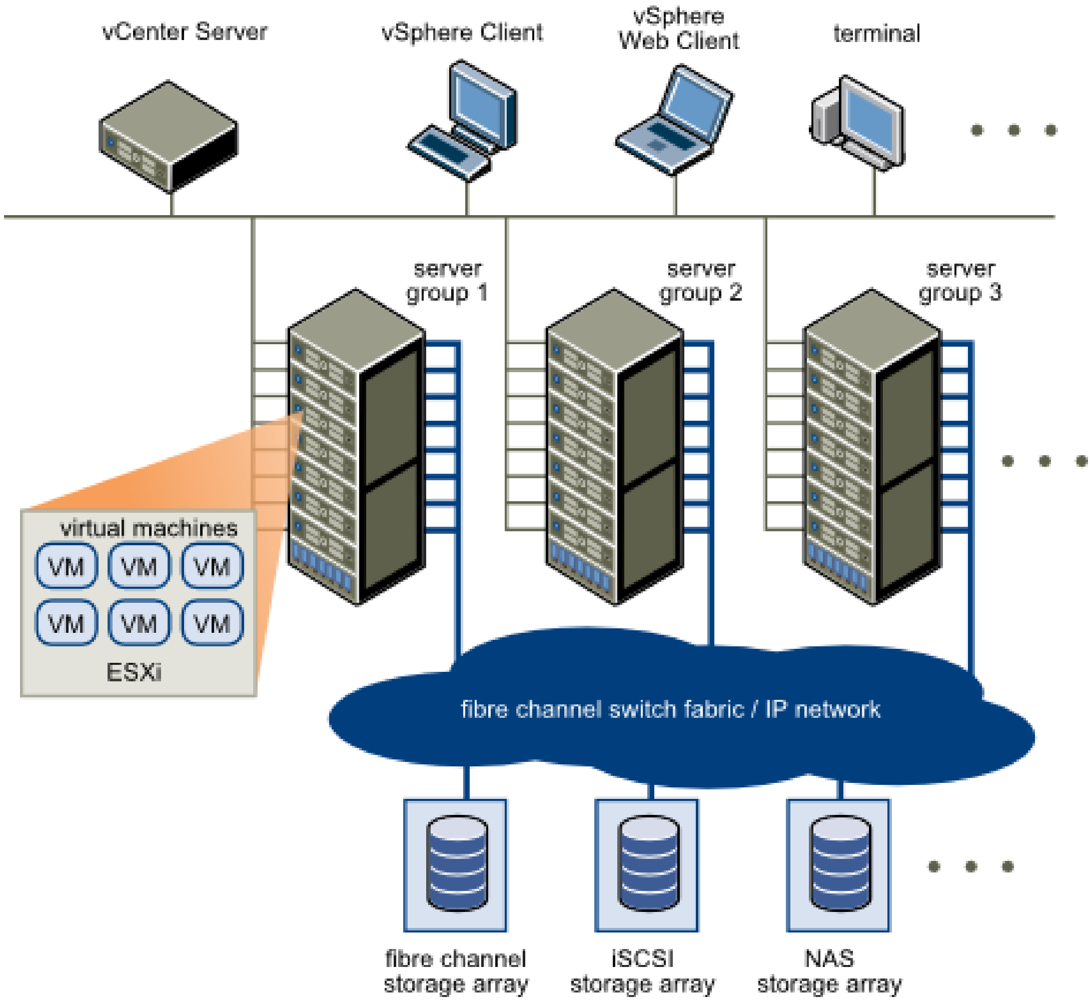
Bare-Metal Hypervisors

Bare-Metal Hypervisors



- A bare-metal hypervisor system does not require an operating system

Virtualized Infrastructure



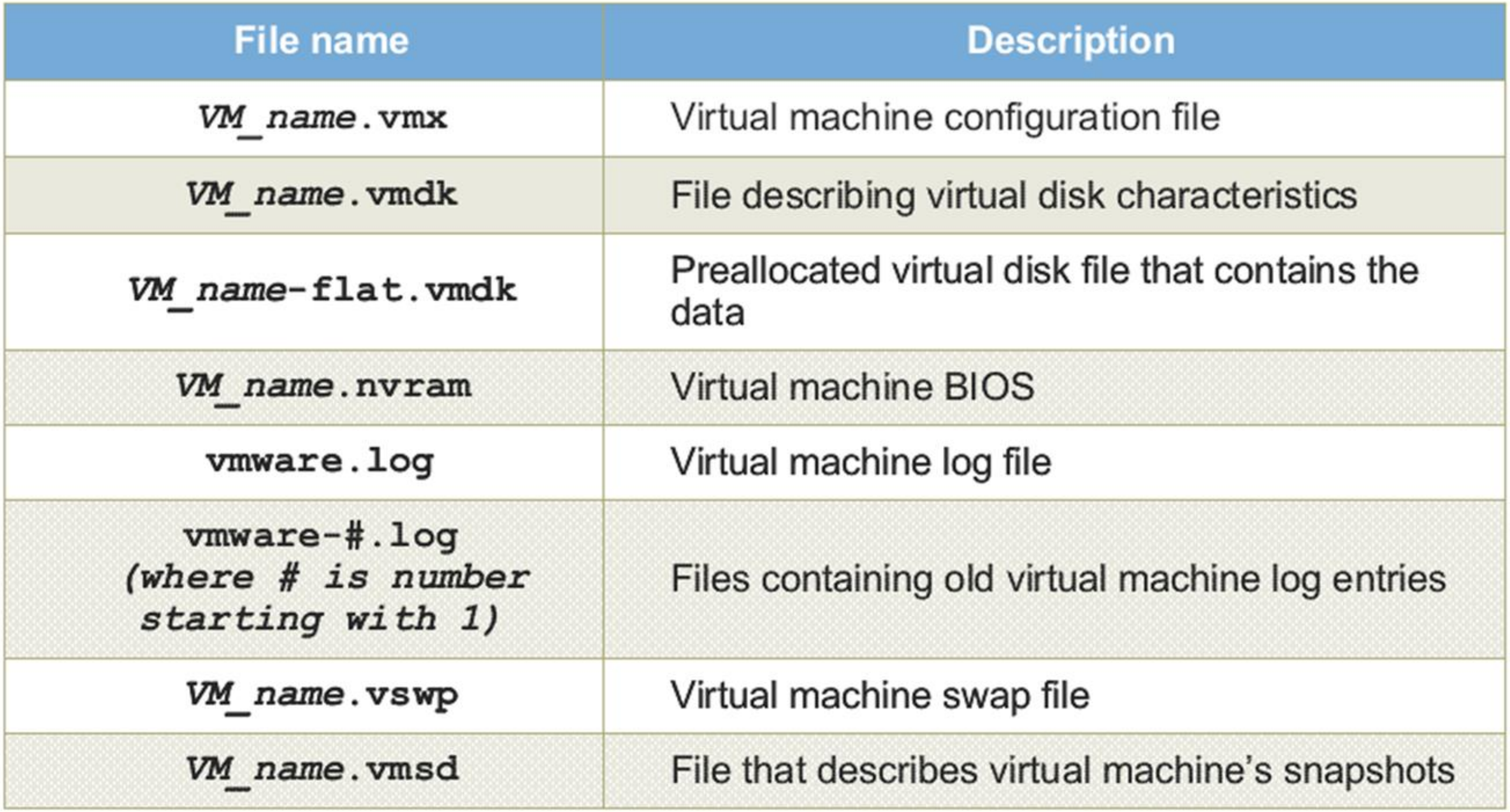
Isolation

- Process Isolation
  - Each virtual machine is completed isolated from the host machine and other virtual machines
- If a virtual machine crashes all others are unaffected
- Network Isolation
  - When allowed VMs can communicate with each other
    - Common network protocols
    - Secure network infrastructure

Encapsulation

- The complete virtual machine environment is saved as a set of files
  - Easy to back up, move and copy
- The VM “box” is described by and stored as a set of specialized files
- All Disk data is file-based
  - Stored in a directory on a datastore that can be accessed by the ESXi server
    - Local Disk
    - FC/iSCSI SAN
    - NFS

Files That Make Up a Virtual Machine



File name	Description
VM_name.vmx	Virtual machine configuration file
VM_name.vmdk	File describing virtual disk characteristics
VM_name-flat.vmdk	Preallocated virtual disk file that contains the data
VM_name.nvram	Virtual machine BIOS
vmware.log	Virtual machine log file
vmware-#.log *(where # is number starting with 1)*	Files containing old virtual machine log entries
VM_name.vswp	Virtual machine swap file
VM_name.vmsd	File that describes virtual machine's snapshots

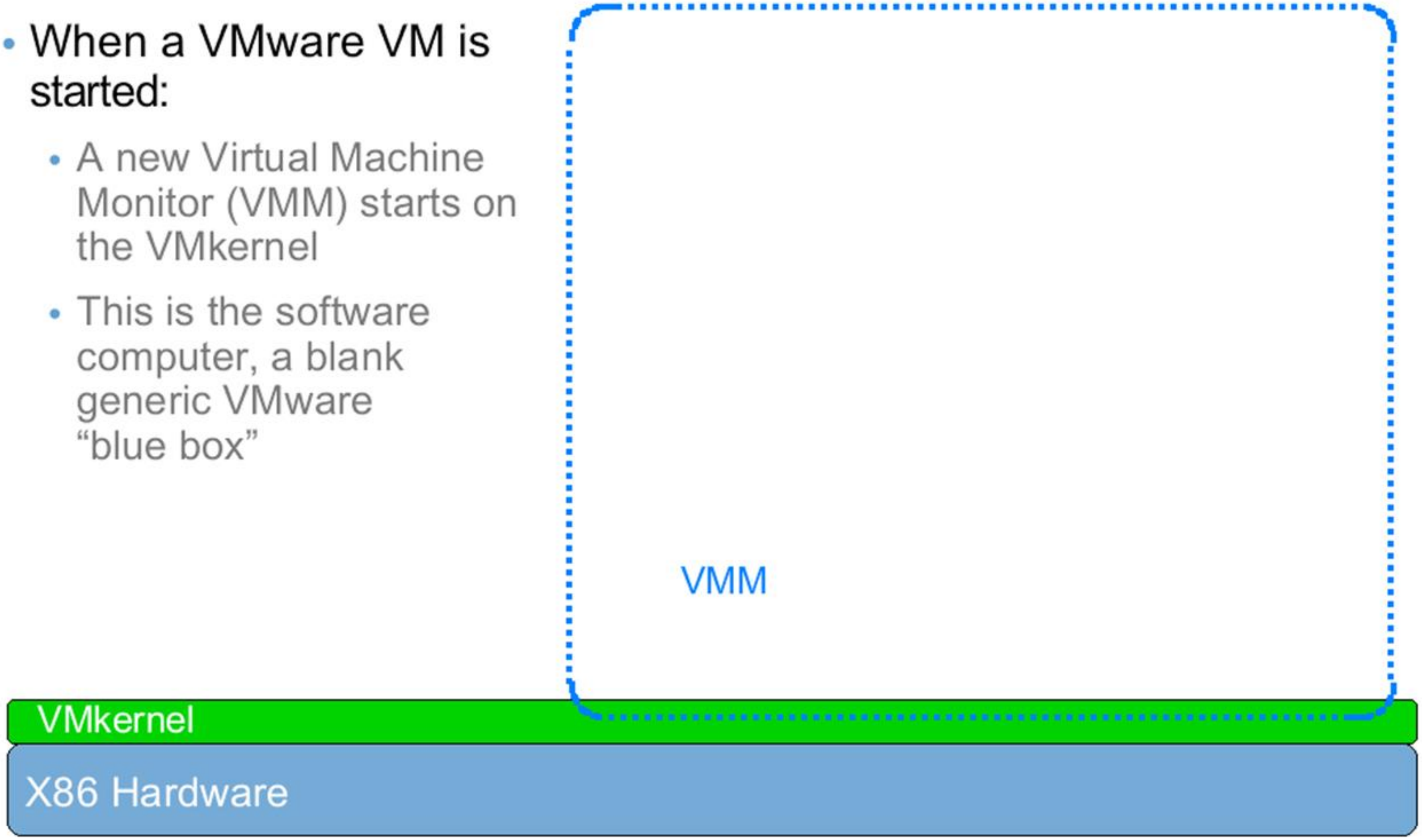
*There are additional files which may appear in a VM's directory

VM Components ESXi

- Similar to the components found in VM-Workstation
- Main Components
  - CPU
  - Memory
  - Storage
  - NIC
- Other Components
  - Floppy
  - CD/DVD
  - Assorted Ports

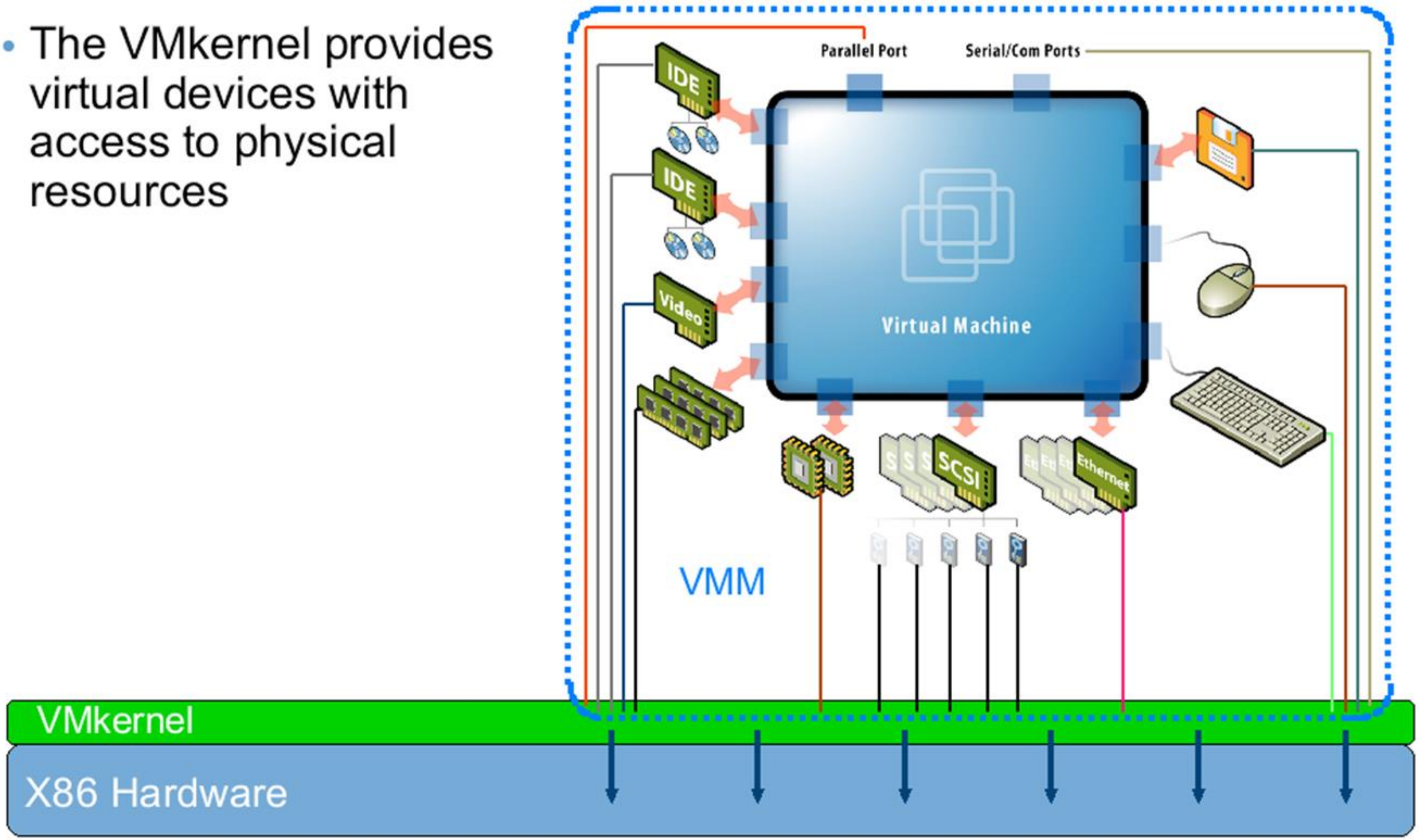
How Virtual Machines Operate

- When a VMware VM is started:
  - A new Virtual Machine Monitor (VMM) starts on the VMkernel
  - This is the software computer, a blank generic VMware "blue box"



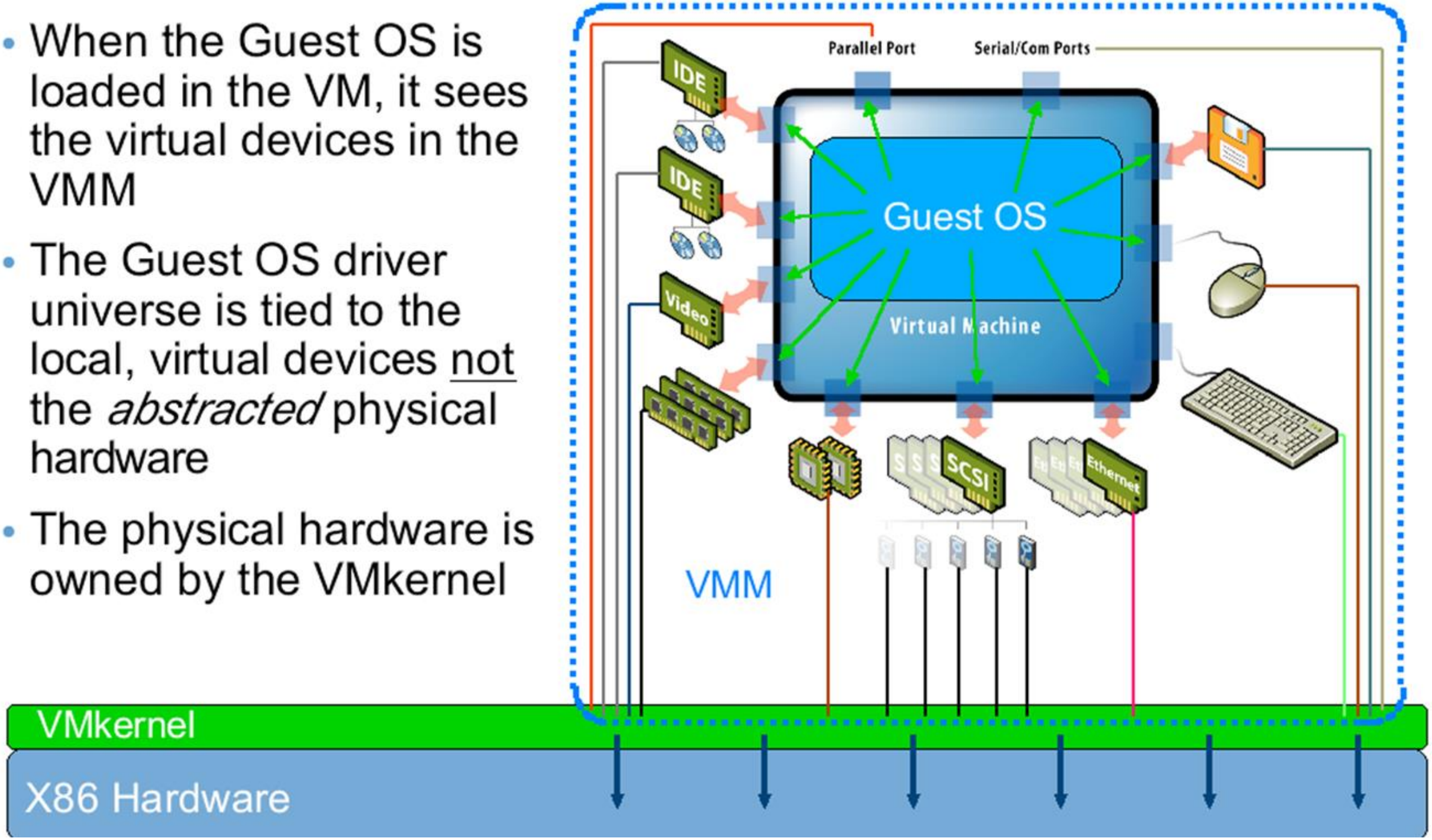
How Virtual Machines Operate

- The VMkernel provides virtual devices with access to physical resources



What The Guest O/S Sees

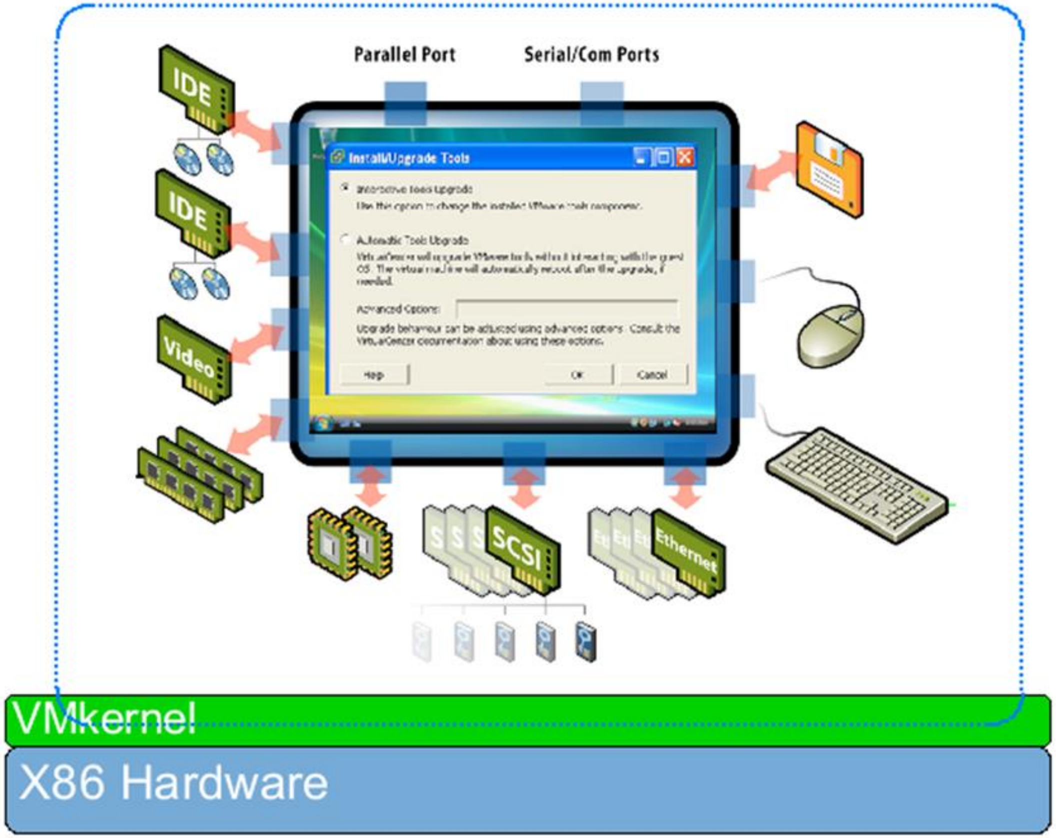
- When the Guest OS is loaded in the VM, it sees the virtual devices in the VMM
- The Guest OS driver universe is tied to the local, virtual devices <u>not</u> the *abstracted* physical hardware
- The physical hardware is owned by the VMkernel



VMWare Tools

Features include:

- Virtual device drivers
- Manual connection and disconnection of some devices while VM is powered on
- Improved mouse
- Memory management
- Support for quiescing a file system
- Time synchronization
- Ability to gracefully shut down virtual machine



Install/Upgrade Tools

● Interactive Tools Upgrade
Use this option to change the installed VMware tools components.

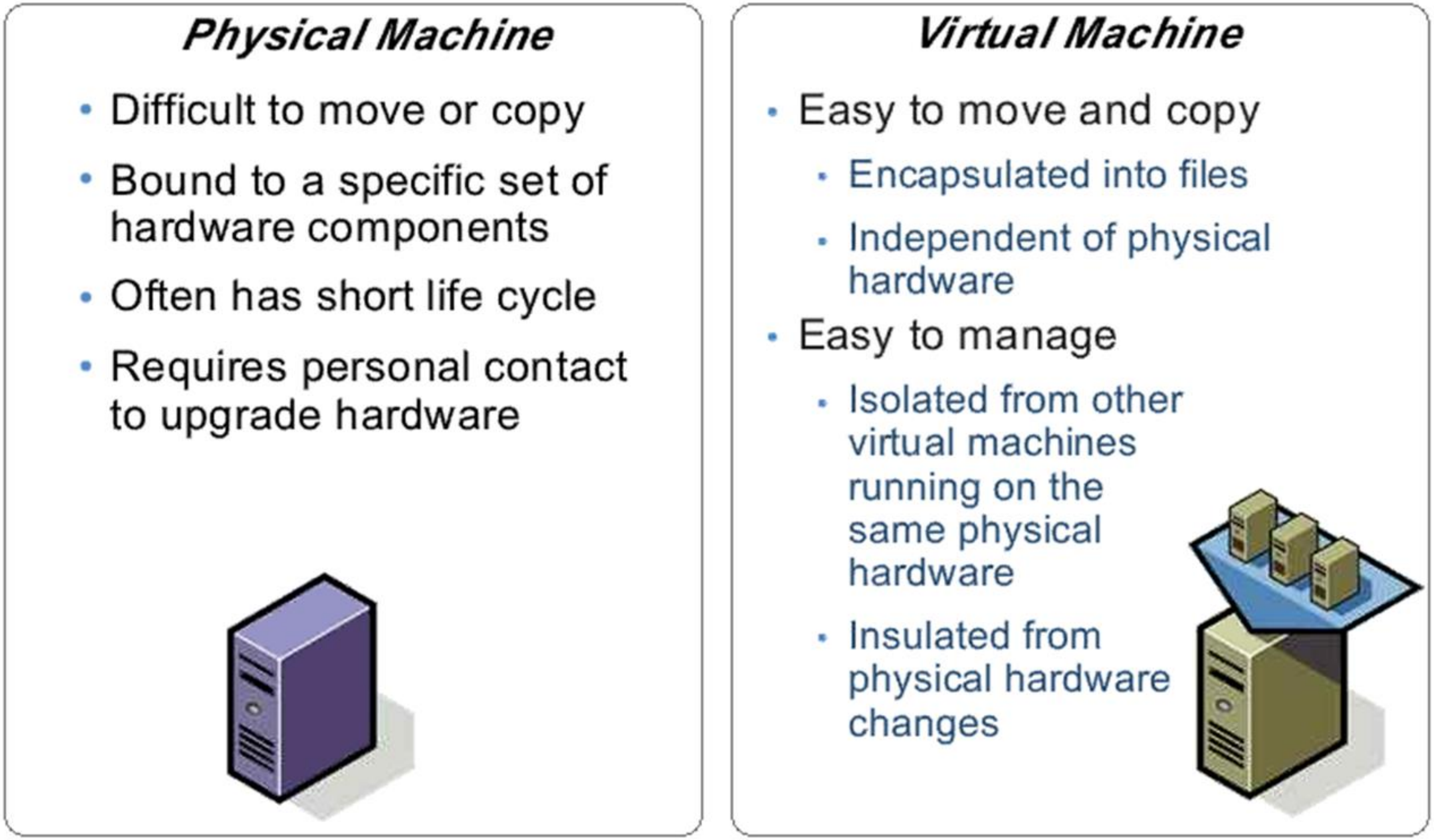
○ Automatic Tools Upgrade
VirtualCenter will upgrade VMware tools without interacting with the guest OS. The virtual machine will automatically reboot after the upgrade, if needed.

Advanced Options:

Upgrade behaviour can be adjusted using advanced options. Consult the VirtualCenter documentation about using these options.

Install into guest OS like an application

Benefits of Virtual Machines



Physical Machine

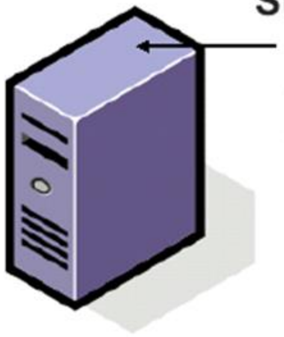
- Difficult to move or copy
- Bound to a specific set of hardware components
- Often has short life cycle
- Requires personal contact to upgrade hardware

Virtual Machine

- Easy to move and copy
  - Encapsulated into files
  - Independent of physical hardware
- Easy to manage
  - Isolated from other virtual machines running on the same physical hardware
  - Insulated from physical hardware changes

Resource Utilization

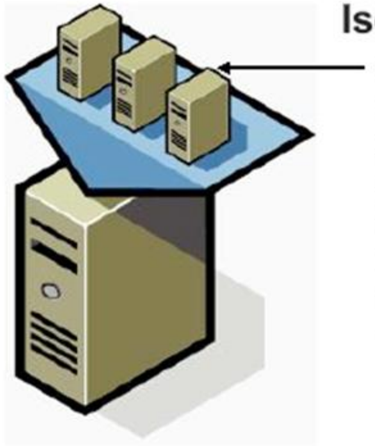
- Physical infrastructure
  - Resource utilization is low
  - Applications don't like to be stacked
  - Encourages sprawl



Stacked applications are unstable at relatively low utilization levels

Virtual infrastructure

- Resource utilization is high
- Isolated VMs don't know/care they're being stacked
- Enables consolidation



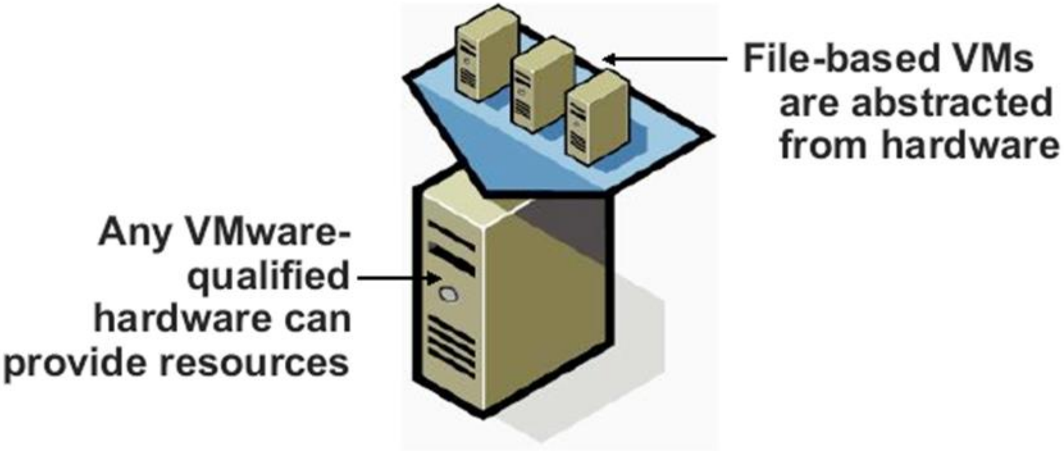
Isolated VMs can be densely stacked and stay stable at high utilization levels

Disaster Recovery

- Physical infrastructure
  - Hardware-specific recovery
  - Disk images

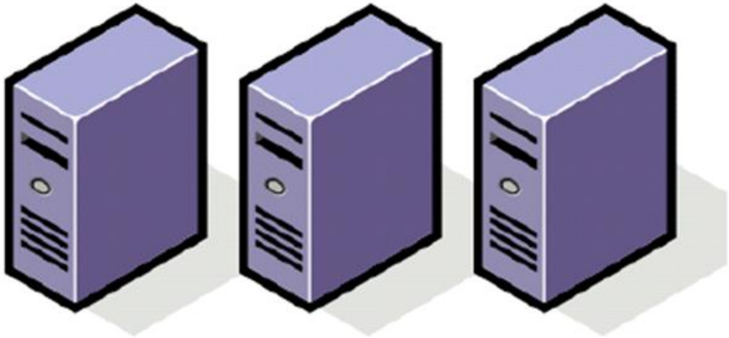
Virtual infrastructure

- Hardware agnostic recovery for VMs
- File-based architecture for recovery (recovery ready by design)


File-based VMs are abstracted from hardware
Any VMware-qualified hardware can provide resources

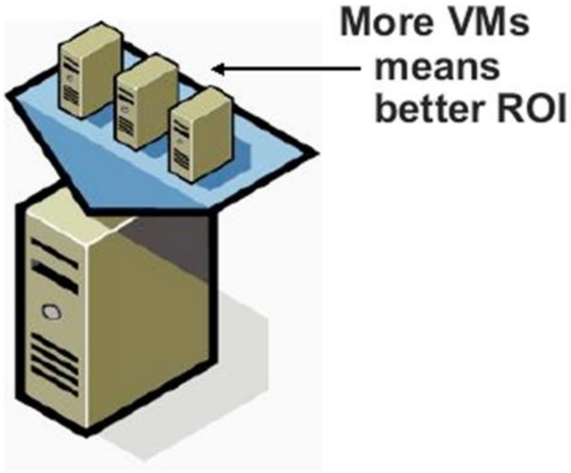
Virtualization & ROI

- Physical infrastructure
  - Hardware is expensive



Virtual infrastructure

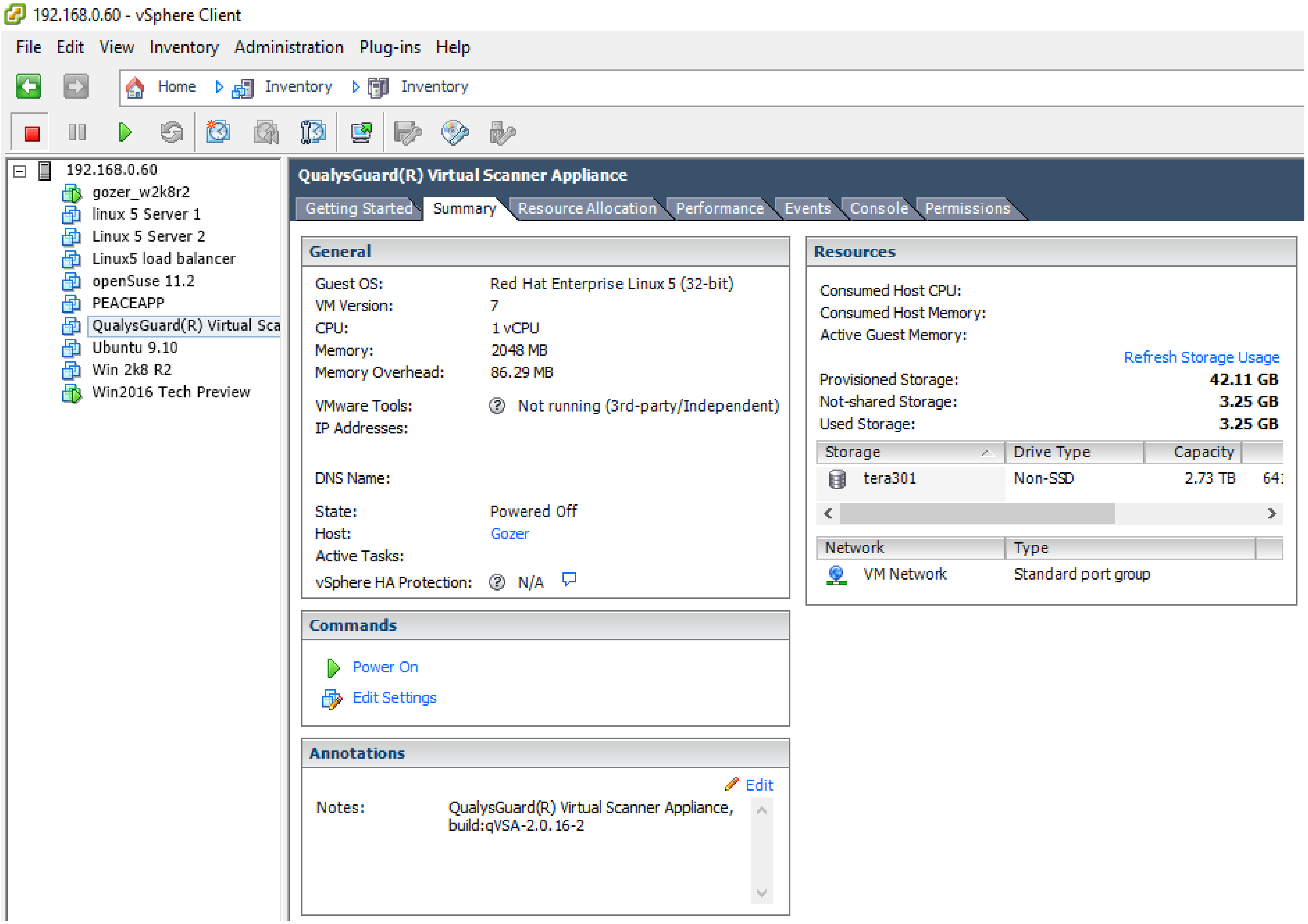
- Consolidation ratios drive ROI in virtualization
- VMware has the best ratios



vSphere Client

- Used to logon to the virtual infrastructure
  - Should be used to log in to the vCenter server
    - Sometimes called vSphere server
  - Can be used to log in to the ESXi hosts
    - Not recommended as it can cause database instability
- vSphere client provides a centralized graphical management interface

vSphere Client



- 192.168.0.60
  - gozer_w2k8r2
  - linux 5 Server 1
  - Linux 5 Server 2
  - Linux5 load balancer
  - openSuse 11.2
  - PEACEAPP
  - QualysGuard(R) Virtual Sca
  - Ubuntu 9.10
  - Win 2k8 R2
  - Win2016 Tech Preview

QualysGuard(R) Virtual Scanner Appliance

General

Guest OS:	Red Hat Enterprise Linux 5 (32-bit)
VM Version:	7
CPU:	1 vCPU
Memory:	2048 MB
Memory Overhead:	86.29 MB
VMware Tools:	Not running (3rd-party/Independent)
IP Addresses:	
DNS Name:	
State:	Powered Off
Host:	Gozer
Active Tasks:	
vSphere HA Protection:	N/A

Commands

Power On

Edit Settings

Annotations

Edit

Notes: QualysGuard(R) Virtual Scanner Appliance, build:qVSA-2.0.16-2

Resources

Consumed Host CPU:
Consumed Host Memory:
Active Guest Memory:

Refresh Storage Usage

Provisioned Storage:	**42.11 GB**
Not-shared Storage:	**3.25 GB**
Used Storage:	**3.25 GB**

Storage	Drive Type	Capacity	
tera301	Non-SSD	2.73 TB	64:

Network	Type
VM Network	Standard port group

Security Areas

- Main components that need to be considered when securing a virtual infrastructure
  - ESXi Hosts
  - vCenter Server
  - VMs
  - Applications Running in the VMs

ESXi Hosts

- Once you have installed ESXi, you won’t normally access the hosts directly, unless:
  - vCenter server is down
  - Or you are troubleshooting boot or configuration issues on the ESXi host
- There are two options for managing authentication
  - Local
  - Active Directory Integration

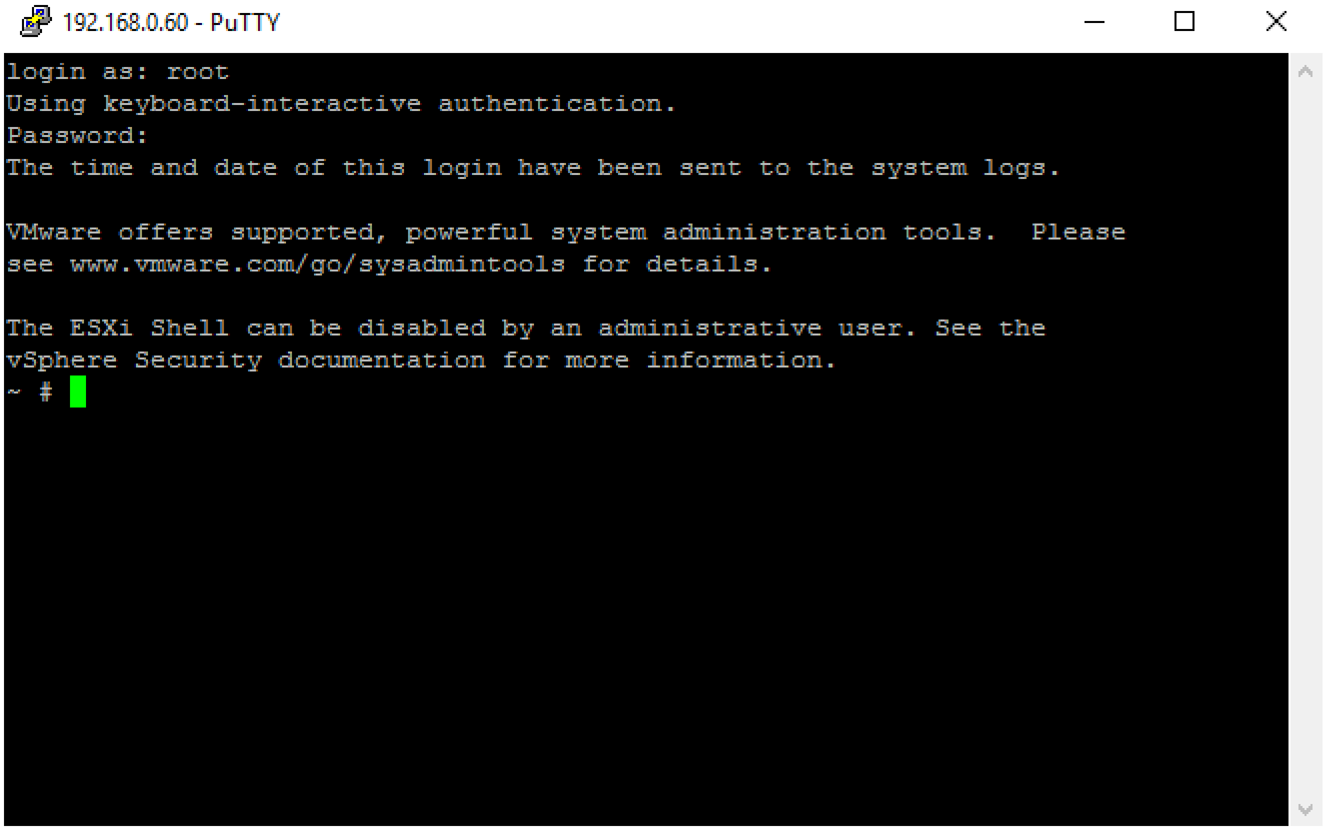
ESXi Hosts

- Local
  - Limit to two or three accounts
  - Need to be configured individually on each host
  - Users can be created locally, by logging into the ESXi host, or through the vSphere client
- Active Directory Integration
  - Allows for the centralized management of user accounts
  - Users can access ESXi hosts through vSphere client or vCLI

ESXi Hosts

- DCUI
  - Direct Console User Interface
  - Provides direct access to the server console
  - Limited to users with the Administrator Role
- CLI access
  - Disabled by default
  - Usually only enabled for support
  - SSH access can be enabled
    - Warning: by default the root login will be able to access the CLI via SSH

ESXi CLI Default Root Login



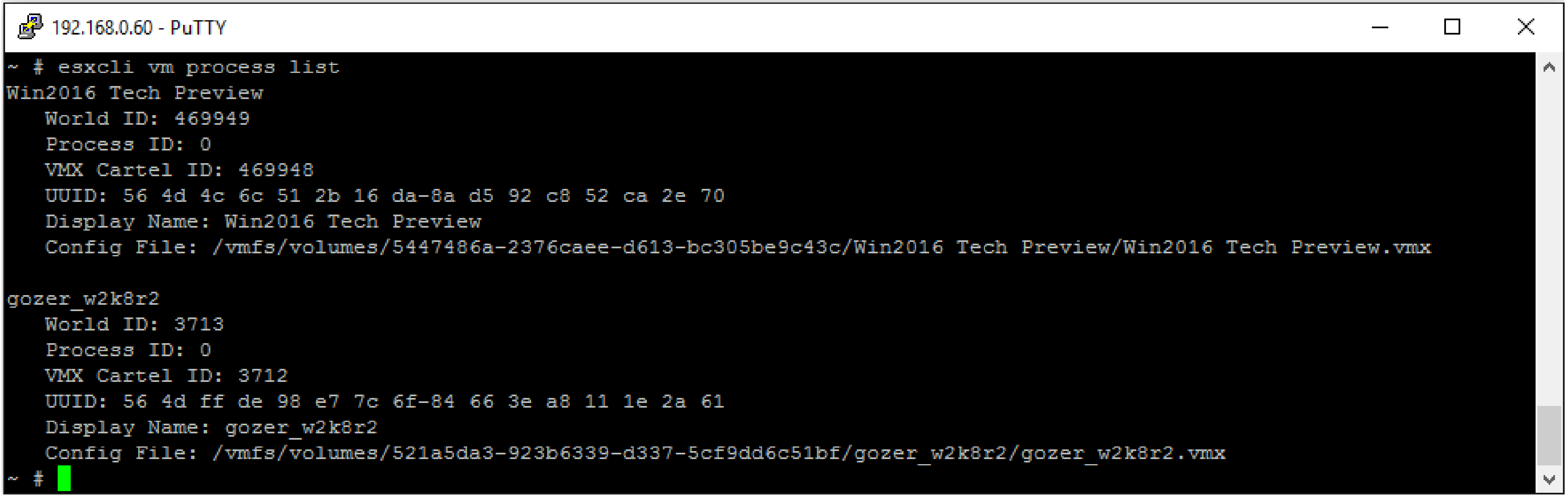
```
login as: root
Using keyboard-interactive authentication.
Password:
The time and date of this login have been sent to the system logs.

VMware offers supported, powerful system administration tools.  Please
see www.vmware.com/go/sysadmintools for details.

The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
~ #
```

ESXi CLI

- The CLI is typically used to troubleshoot VMs
- Has many commands to assist in remote troubleshooting sessions



```
~ # esxcli vm process list
Win2016 Tech Preview
   World ID: 469949
   Process ID: 0
   VMX Cartel ID: 469948
   UUID: 56 4d 4c 6c 51 2b 16 da-8a d5 92 c8 52 ca 2e 70
   Display Name: Win2016 Tech Preview
   Config File: /vmfs/volumes/5447486a-2376caee-d613-bc305be9c43c/Win2016 Tech Preview/Win2016 Tech Preview.vmx

gozer_w2k8r2
   World ID: 3713
   Process ID: 0
   VMX Cartel ID: 3712
   UUID: 56 4d ff de 98 e7 7c 6f-84 66 3e a8 11 1e 2a 61
   Display Name: gozer_w2k8r2
   Config File: /vmfs/volumes/521a5da3-923b6339-d337-5cf9dd6c51bf/gozer_w2k8r2/gozer_w2k8r2.vmx
~ #
```

ESXi Hosts

- Firewall
  - Controls inbound and outbound network traffic
  - By default it only allows traffic managing the ESXi hosts and the VMs running on them
  - Can be used to control which IP or IP ranges have access to the management interfaces
- Patching
  - As with any other system you need to keep the hosts patched
  - vSphere update manager can be used to keep the entire environment up to date

Securing vCenter Server

- Deals mostly with securing the underlying OS
- There are two version of vCenter Server
  - Windows Server Based version of vCenter
    - Regular Window security measures
  - SUSE Linux virtual appliance
    - Preconfigured Linux instance that doesn’t provide many options for further configuration or patching

- Note: the vCenter server version must match the vSphere client version
  - e.g. 5.1 and 5.1

Securing vCenter Server

- Windows Based Version (on top of regular measures)
  - Current vCenter Server patches and updates
  - Keep vCenter Server backend database on a separate system (isolation)
  - Use a dedicated service account if you are using Windows authentication with SQL server
  - Replace the default SSL certificate with a valid SSL certificate from a trusted authority

Security Model

- User or Group
  - Authentication Mechanism
- Privilege
  - Action that can be performed on an object in the inventory
- Role
  - Combination of a user or group with a collection of privileges
- Permission
  - Assignment of a role to an inventory object

Standard Security Model

- Like most environments we use a combination of Subjects, Objects and Access Controls to control access
- **Subjects**: Users and Groups
- **Objects**: Inventory Objects
- **Access Controls**: Privileges, Roles and Permissions

Note: In the labs an inventory object refers to a VM

Security Model

- Security Model Basics
  - Users/Groups are assigned to a role
  - The role has associated privileges
  - The user-role-privilege combination is associated with an object in the inventory as a permission
- There are three default roles
  - No Access
  - Read Only
  - Administrator

Default Roles

- No Access
  - Works as the name suggests
  - Particularly useful to restrict access further down the hierarchy
    - Admin access to ESXi host, but no access to a specific VM
- Read Only
  - Allows the user to see the objects in the inventory, but they can’t interact with them
- Administrator
  - Has the utmost authority

Roles Continued

- Custom Roles
  - Allow for more granular control
- vSphere Cient’s Role View
  - Allows administrators to identify where roles have been assigned and what permissions have been granted in the inventory

ESXi Host Logging

- Every ESXi host runs a syslog daemon that captures events for future reference
  - – Stored locally in a 4GB scratch disk by default
  - – Difficult to interact with
- More common solution is to send the logs to a syslog server
  - – VMware Syslog Collector needs to be installed to enable this functionality

Securing VMs & Applications

- Deals with securing the underlying OS and applications running within the OS
  - Keeping everything patched
- The main vSphere specific measures deal with Network Security Policies
  - Particularly useful when using the vSphere distributed switch of Cisco’s Nexus switch
  - Allow for more granular control of network traffic
  - Similar controls to those of real world switches

Key Security Concepts

- Configure and Control Authentication
- Manage Roles and Access Controls
- Control Network Access to services on ESXi hosts
- Integrate with Active Directory

VMWare Security Resources

- Provides official notifications of security related vulnerabilities
- Also has a number of configuration guides that provide valuable information

http://vmware.com/security/advisories

Practical uses for VMs

- The ability to run older Operating Systems on top of your current O/S for testing or using older software
- Testing new Operating Systems without having to install them on your main machine or a production server
- Testing Malware infections to determine the effect they have on the system

Practical uses for VMs

- Using a headless server to push out different Virtual Machines to multiple users
- Will require a CPU with VT-D technology to pass PCI devices to Virtual Machines
- GPUs and Soundcards, as well as USB devices can be passed through to Workstations

Some Hypervisor Options

- Lime Tech unRAID

https://lime-technology.com/

- VMWare ESXi

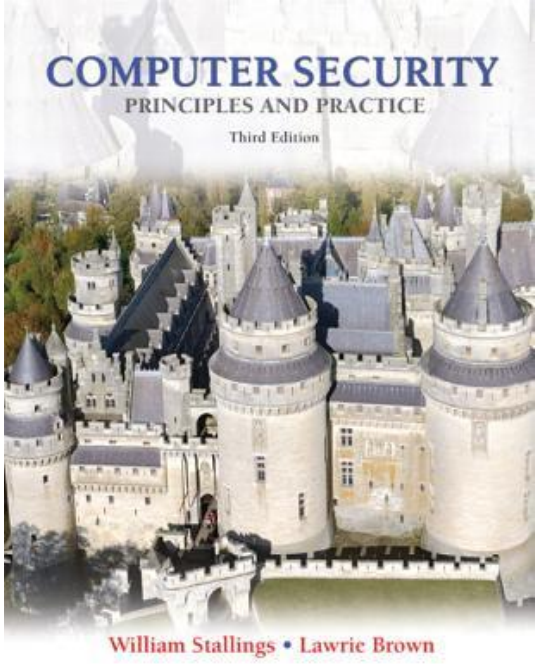
http://www.vmware.com/ca/en/products/esxi-and-esx

- Citrix XenApp

https://www.citrix.com/products/xenapp/overview.html

Homework

- Read Chapter 12 Sections:
- 12.8 – Virtualization Security
- 12.9 – Recommended Reading
- 12.10 – Key Terms & Review Questions



Lab 10 – vSphere Client

Lab 8 Details

- Create ESXi VM in Vmware Workstation 12
- Install vSphere Client on guest Windows 7 VM
- Create Users & Assign Permissions
- Create Resource Pools & Assign Roles
- Configure Shell Access with SSH