CSec15233
Malicious Software Analysis

Malware Analysis in Virtual Machines

Qasem Abu Al-Haija

Introduction

- Dynamic Analysis (DA):
  - requires running malware deliberately while monitoring the results.
- This requires setting up a safe environment.
  - Allow investigating malware without exposing your machine or network to unexpected risk.
- Must prevent malware from spreading to production machines.
  - You can use dedicated real or virtual machines to study malware safely.

Real machines

- Real machines (RM) can be air-gapped.
  - no network connection to the Internet or to other machines
- Disadvantages
  - No Internet connection, so parts of the malware may not work
  - Can be difficult to remove malware, so re-imaging the machine will be necessary.
- Advantages
  - Some malware detects virtual machines and won't run properly in one.

Virtual machines

- Virtual machines (VM):
  - like a computer inside a computer
  - The most common method
  - We'll do it that way

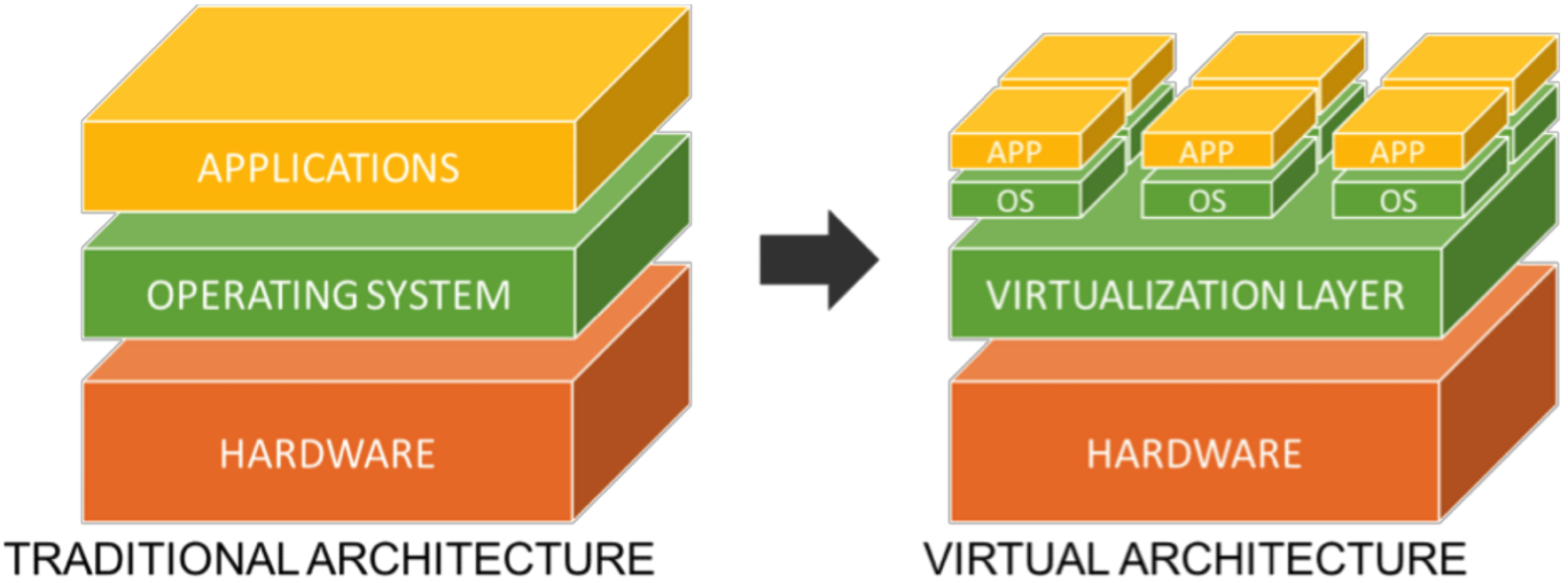
- This protects the host machine from the Malware
  - Except for a few very rare cases of malware that escape the virtual machine and infect the host

Overview of Virtualization

Understanding the Basics of Virtualization

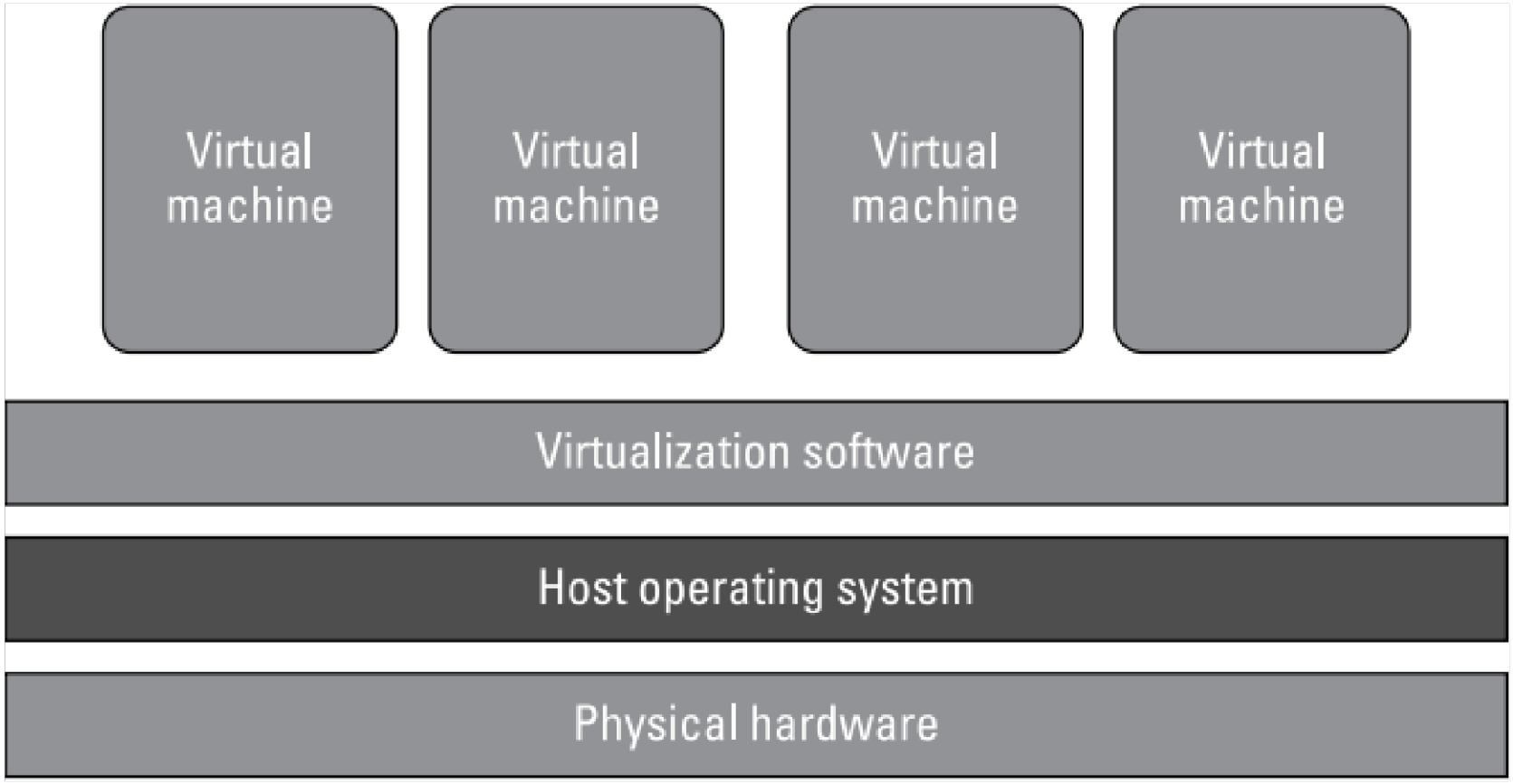
- Virtualization is the process of using computer resources to imitate platform resources to increase IT resource utilization, efficiency, and scalability.
  - Accessing, storing, analyzing, and managing malware in isolated environments.
  - Can be applied across the entire IT infrastructure, including SW, HW, and networks.
- Virtualization separates resources & services from the underlying physical environment.
  - Enabling you to create many virtual systems within a single physical system.
- Although virtualization adds a huge amount of efficiency➔ it doesn't come without a cost.
  - Virtual resources must be secured against intruders with regular deleting of unused images

Understanding the Basics of Virtualization



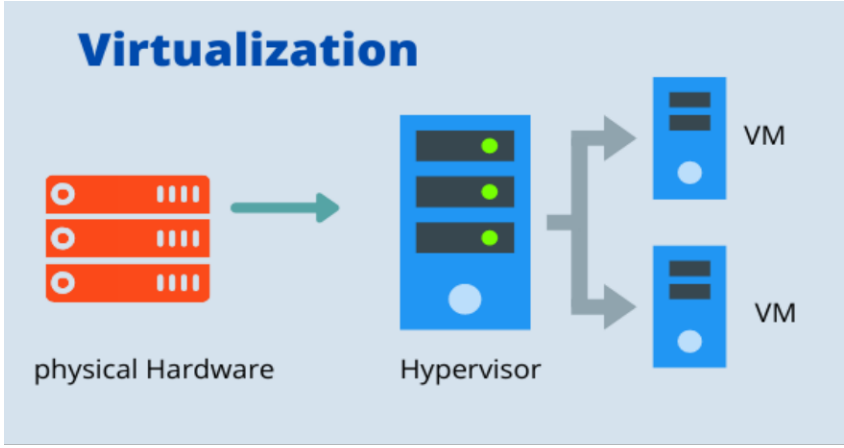
Typical virtualization environment

Using virtualization software to create several virtual systems within a single physical system



How virtualization works

- ✓ A SW component hypervisor is installed on the physical machine.
- ✓ Hypervisor creates virtual platforms on the physical machine on top of which multiple OSs are installed and monitored
- ✓ These virtual platforms are called virtual machines (VMs).
- ✓ Hypervisor is also called Virtual machine monitor (VMM).
- ✓ Guest OS is then installed on this VM, and the guest OS sees VM as if they are its native, actual hardware components
- ✓ Now your apps run on these Guest OS



Primary reasons to implement virtualization

- Improve the efficiency of processing a diverse mix of workloads.
  - Pool of virtual resources allows companies to improve latency.
- Instead of assigning dedicated physical resources to each task.
  - Pool of virtual resources can be quickly allocated across all workloads.
- Isolated/safe environment to run/investigate insecure applications
  - Such as the malware analysis process.

Primary benefits to implement virtualization

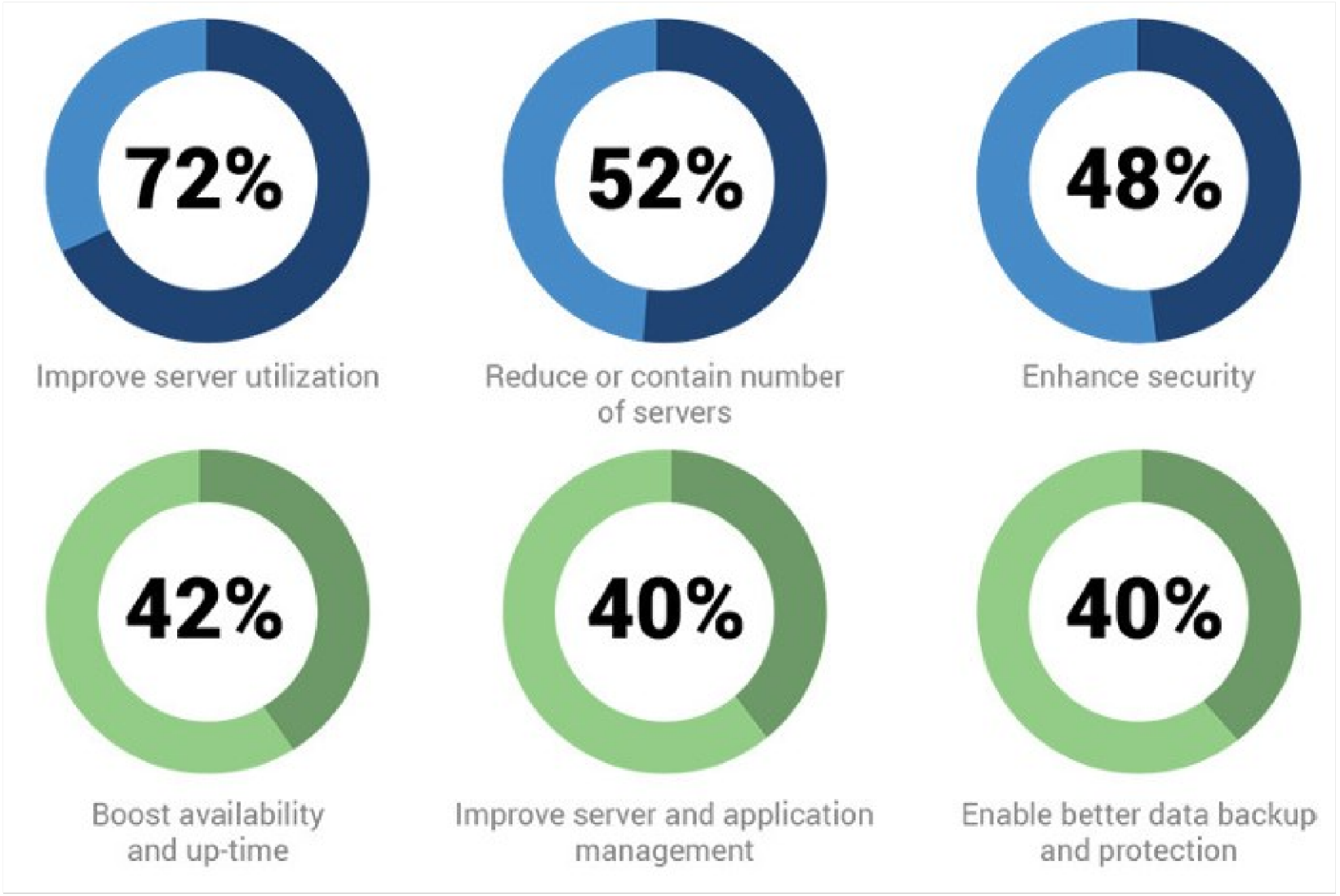
- Virtualization of physical resources has substantially improved their utilization.

- Virtualization improved the control and security over the usage and performance of IT resources.

- Virtualization provides automation & standardization to optimize the computing environment.

- Virtualization provides a foundation for cloud computing.

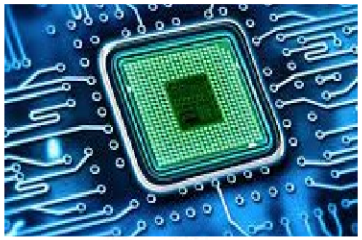
Primary benefits to implement virtualization



Main Characteristics of Virtualization

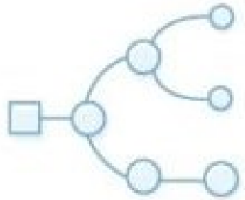
- **Partitioning:**
  - ✓ Many Apps/OSs are supported by partitioning the available resources.
- **Isolation:**
  - ✓ Each VM is isolated from its host physical system and other VMs.
- **Encapsulation:**
  - ✓ A VM can be represented as a single file (image) to be easily identified.
- **Abstraction:**
  - ✓ Hiding the details about the underlying physical delivery environment.
  - ✓ No need for users to worry about the actual locations of data elements.

Types of virtualization

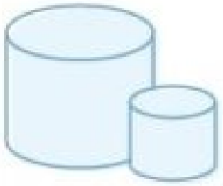


Processor

Data



Network



Storage

Server

Application

Memory

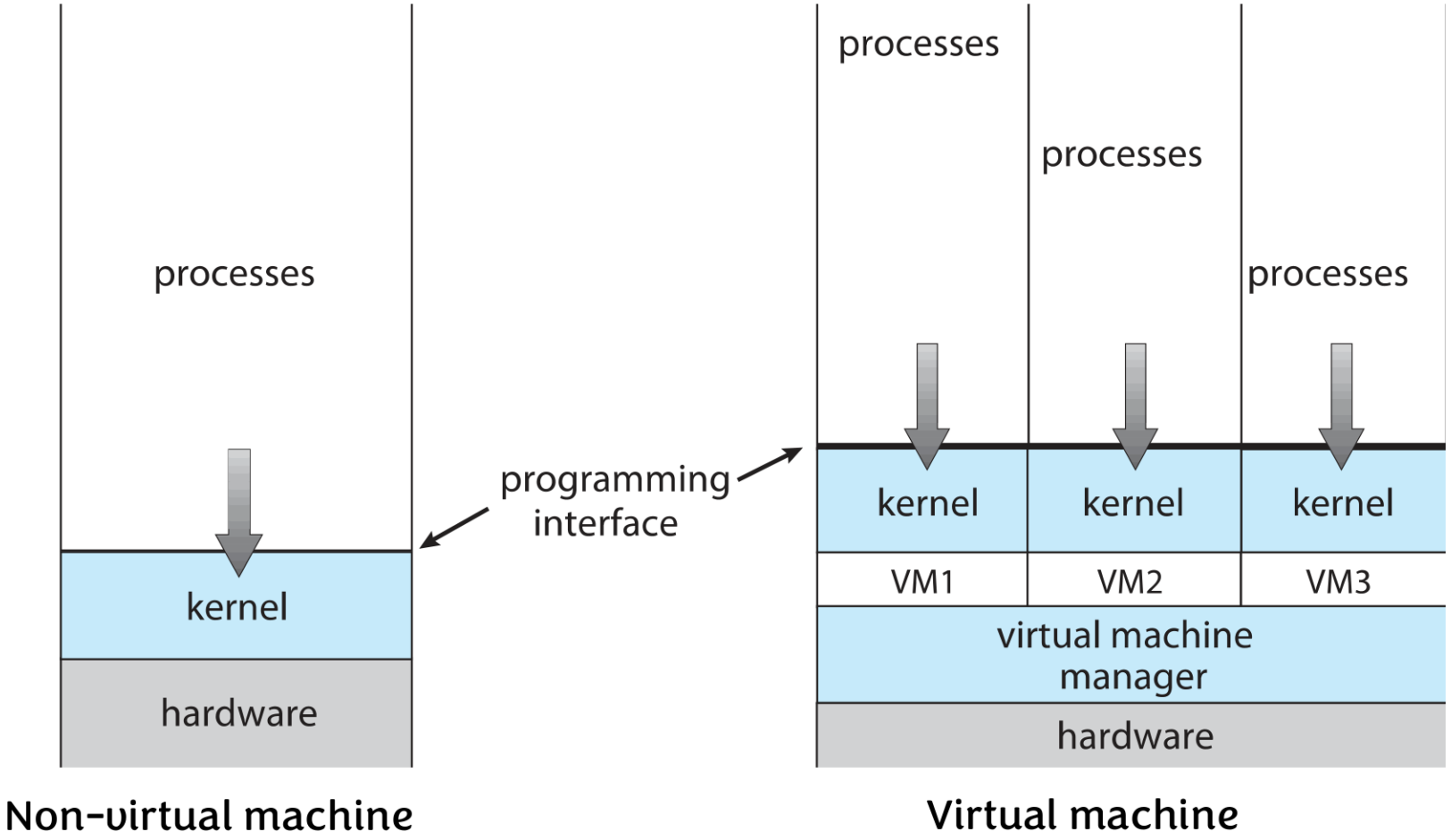
Virtual Machines for Malware Analysis

Virtual Machines

- **What is a virtual machine?**
  - Simply, a computer in your computer
  - Isolated virtual environment that emulates real hardware
  - There are different types/methods

- **Several components**
  - **Host** – underlying hardware system
  - **Virtual machine manager** (**VMM**) or **hypervisor** – creates and runs virtual machines
  - **Guest** – process provided with a virtual copy of the host, usually an operating system

System Models



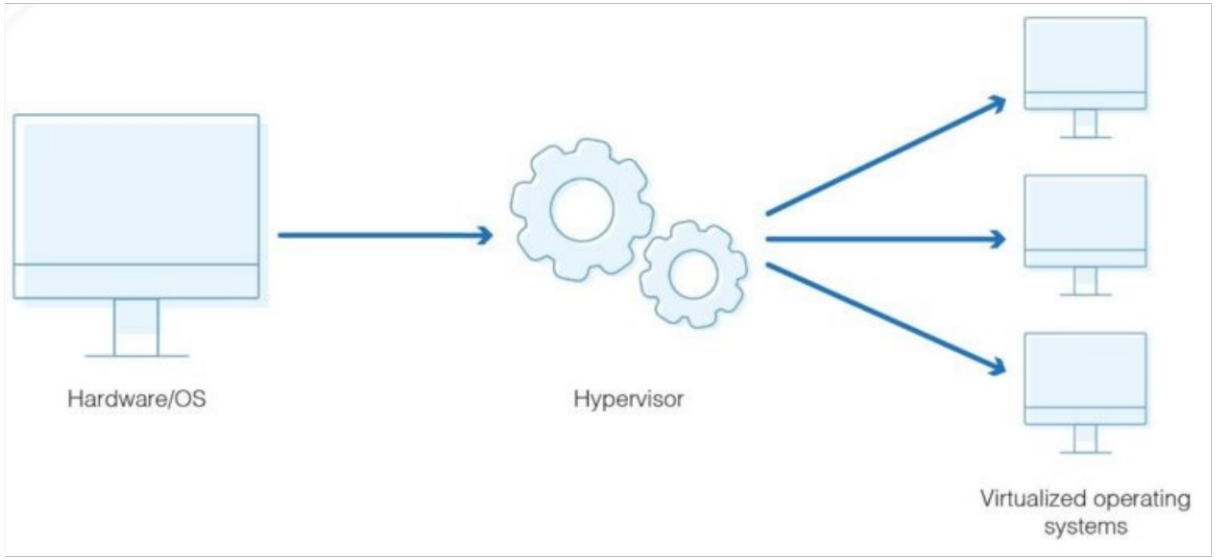
Non-virtual machine

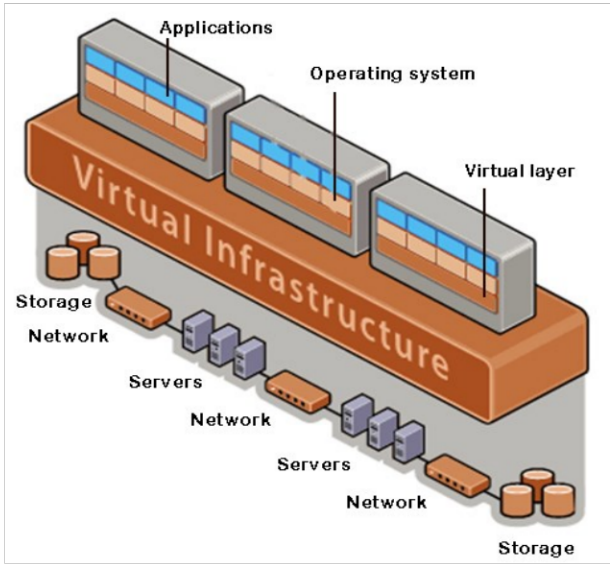
Virtual machine

Implementation of Hypervisor (VMMs)

❑ What is Hypervisor?

- Technology to ensure dynamic resource sharing in ordered & repeatable way.
- Allows multiple OSs to share a single host by creating and running VMs.
- Located at the lowest levels of the hardware environment (fabric layer).
- Hypervisor supports many different operating environments.

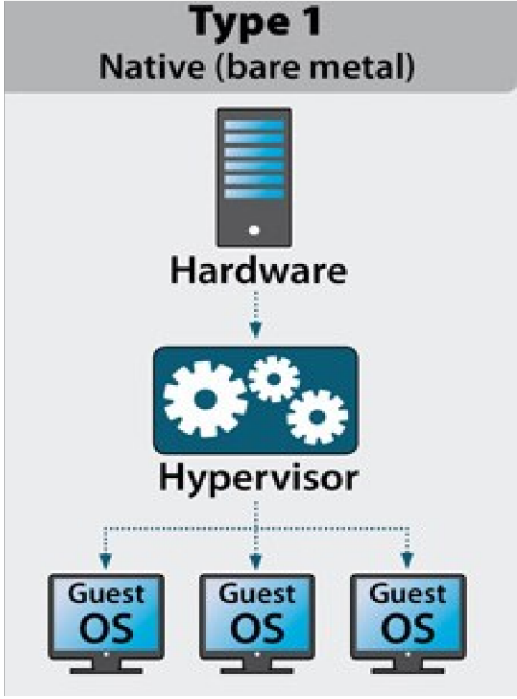




Implementation of Hypervisor

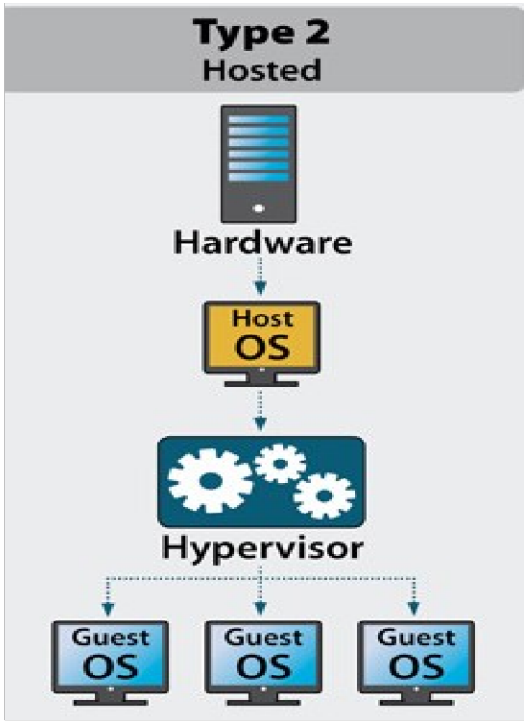
❑ Type 1 hypervisors

- run directly on the HW platform (OS-like SW).
- They achieve higher efficiency because they're running directly on the platform.
- Such as VMware ESX and Citrix XenServer.



❑ Type 2 hypervisors

- run on the host OS.
- They are often used when a need exists to support a broad range of I/O devices.
- such as VMware Player, Fusion, and Oracle VirtualBox

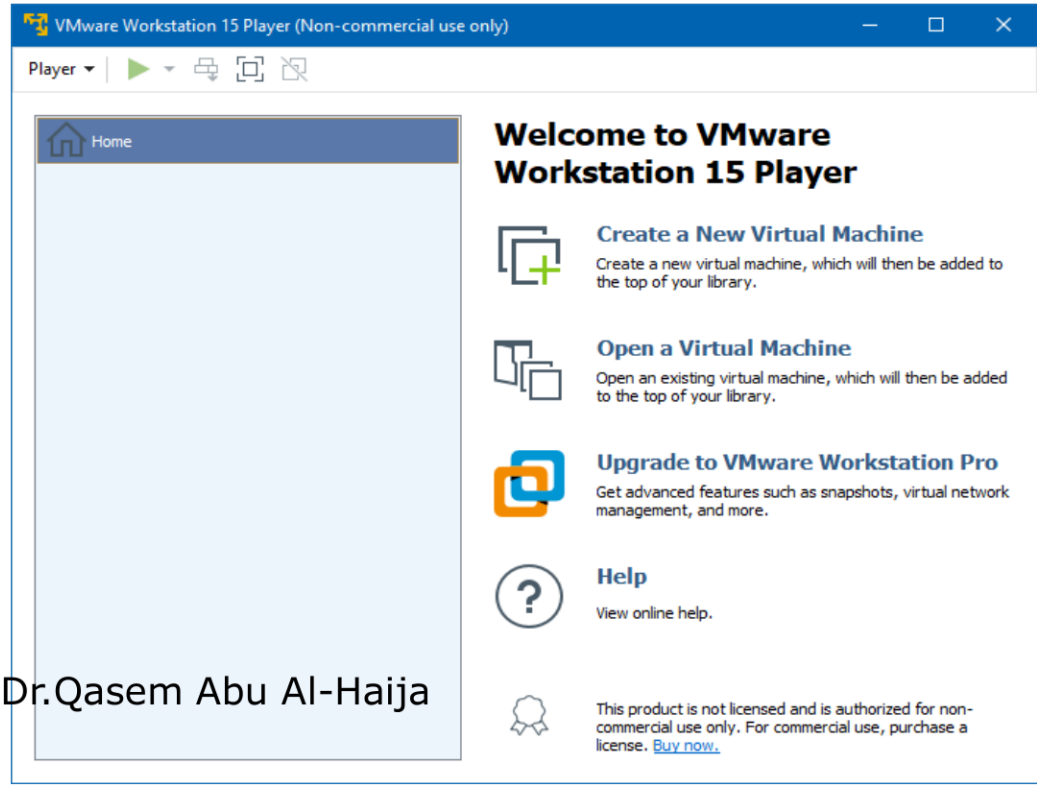


Why are we using a VM?

- Safety, reliability, consistency, it's easy
- Keep the malware in a contained environment
- Snapshots: completely 100% revert the VM to an earlier state
- If things go bad, no one cares

VMware Player

- Free but limited
- Cannot take snapshots
- VMware Workstation or Fusion is a better choice, but they cost money
- Allows for drag and drop between host and guest.
- You could also use VirtualBox, Hyper-V, Parallels, or Xen



Some characteristics of VMware

- Intelligent disk allocation: resize its virtual disk dynamically based on your storage need.

- Improves the user experience by making the mouse and keyboard more responsive.

- Allows access to shared folders, drag-and-drop file transfer, and other useful features.

Basic Steps

- Download and Install VMware player 16.
- Choose the hard drive size based on your needs.
  - A virtual drive size of 20GB is typically a good beginning.
- Install the required OS.
  - Most malware and malware analysis tools run on Windows.
- Install required applications for Malware analysis
- Configure Vmware Player and the virtual OS.
- Take a snapshot (Clean State).

Windows XP

- The malware we are analyzing targets Windows XP, as most malware does
  - Alternatively: You can use Windows Server 2008

- We will use VMware Player with a Windows XP environment.
  - Follow How to add an XP Mode Virtual Machine to Windows 10 (or 11) using VMWare Player

- Within Windows XP to access the Internet
  - Use IE to go to www.bing.com
  - Search Firefox, download and install it
  - Firefox can access any website, while IE cannot!

Configuring VMware Player

- Most malware includes network functionality.
  - E.g.: a worm performs network attacks against other machines to spread itself.
  - But you would not want to allow worm access to your network because it could spread to other computers.
  - So, you may want to disconnect the Network while analyzing worms

- When analyzing malware, you may want to observe the malware's network activity.
  - This helps you understand the author's intention to create signatures or to exercise the program fully.
  - VMware offers several networking options for virtual networking.

Configuring VMware Player

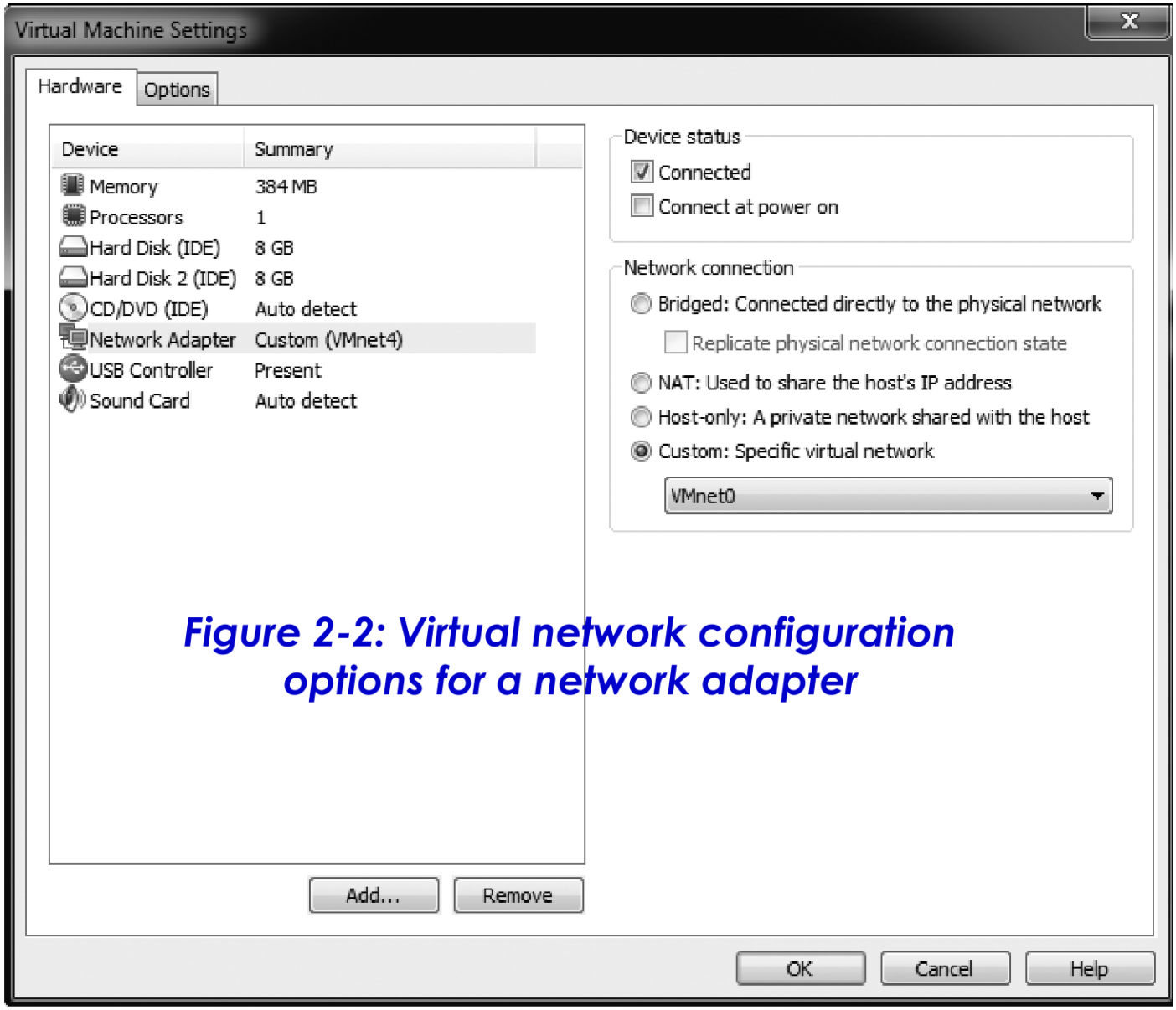


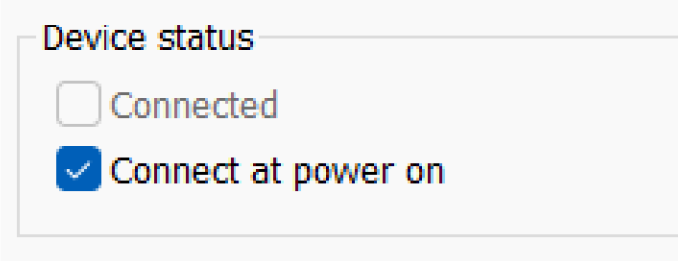
Figure 2-2: Virtual network configuration options for a network adapter

Disconnecting the Network

- You can configure a VM to have no network connectivity.
  - This is not a good idea to disconnect the network, except for certain cases.
  - In this case, you can not analyze malicious network activity.

- However, you can disconnect the network either by
  - Removing the network adapter from the VM or by
  - Disconnecting network adapter by choosing VM Removable Devices.

- You can also control network connectivity whether :
  - Network adapter is connected automatically when the machine is turned on
  - Or by checking the “Connect at power on” check box.



Host-only networking

- Host-only networking creates a separate private LAN between the host OS and the guest OS.
- Host-only networking allows network traffic to the host but not the Internet.
- Make sure that your host is fully patched as protection in case the malware you're testing tries to spread.

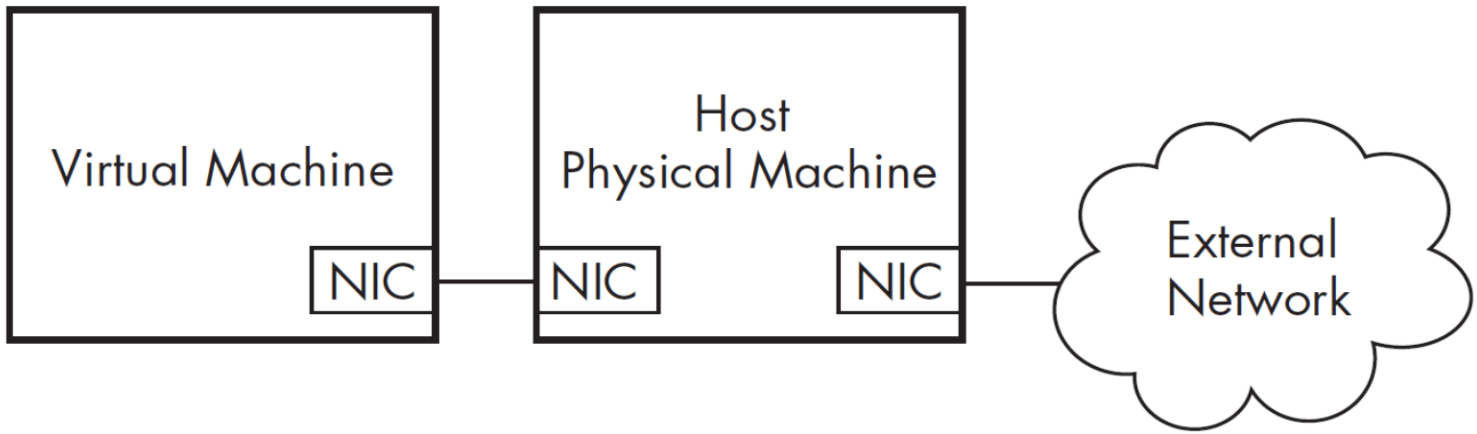


Figure 2-3: Host-only networking in VMware

Using Multiple VMs

- Multiple VMs linked by a LAN but disconnected from the Internet and host machine
- So that the malware is connected to a network without being connected to anything important.
- Figure 2-4 shows a custom network with two VMs connected.
  - The first VM is set up to analyze malware
  - The second VM provides services.
  - Both are connected to a virtual switch "VMNet".

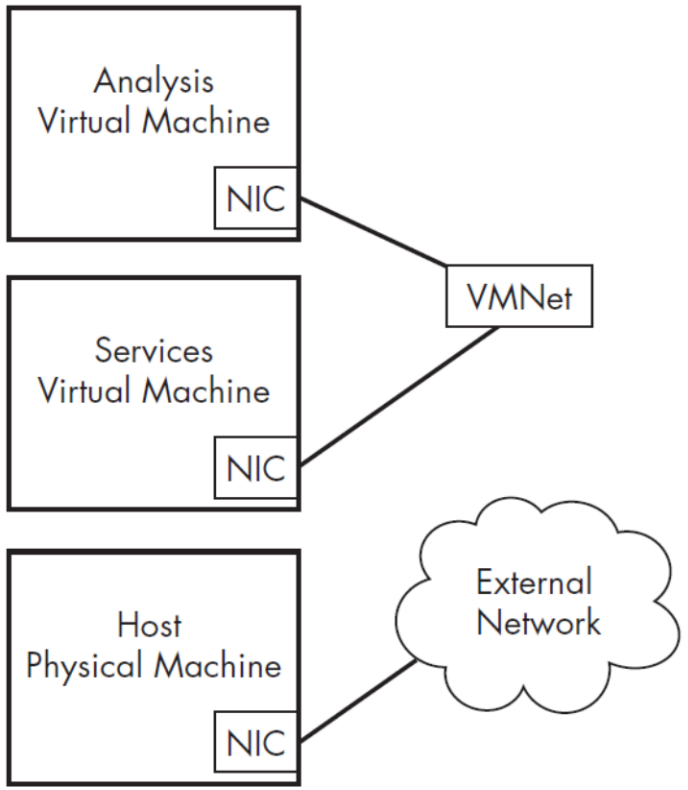


Figure 2-4: Custom networking in VMware

Using Your Malware Analysis VM

- To better exercise the malware analysis subject:
  - it's better to simulate all network services on which the malware relies.
- For example:
  - Malware commonly connects to an HTTP server to download additional malware.
  - To observe this activity, the malware needs access to a DNS server to resolve the server's IP address, as well as an HTTP server to respond to requests.
- Therefore, for efficient Malware Analysis using VM:
  - Connecting Malware to the Internet
  - Connecting and Disconnecting Peripheral Devices
  - Taking Snapshots
  - Transferring Files from a Virtual Machine

Connecting Malware to the Internet

- Sometimes needed to provide a more realistic analysis environment, despite the obvious risks.

- **Two major risks:**
  - Your computer will perform malicious activity, such as:
    - Spreading malware, sending spam, or participating in a DDoS attack.
  - Malware writer could notice that you are connecting to the malware server and trying to analyze the malware.

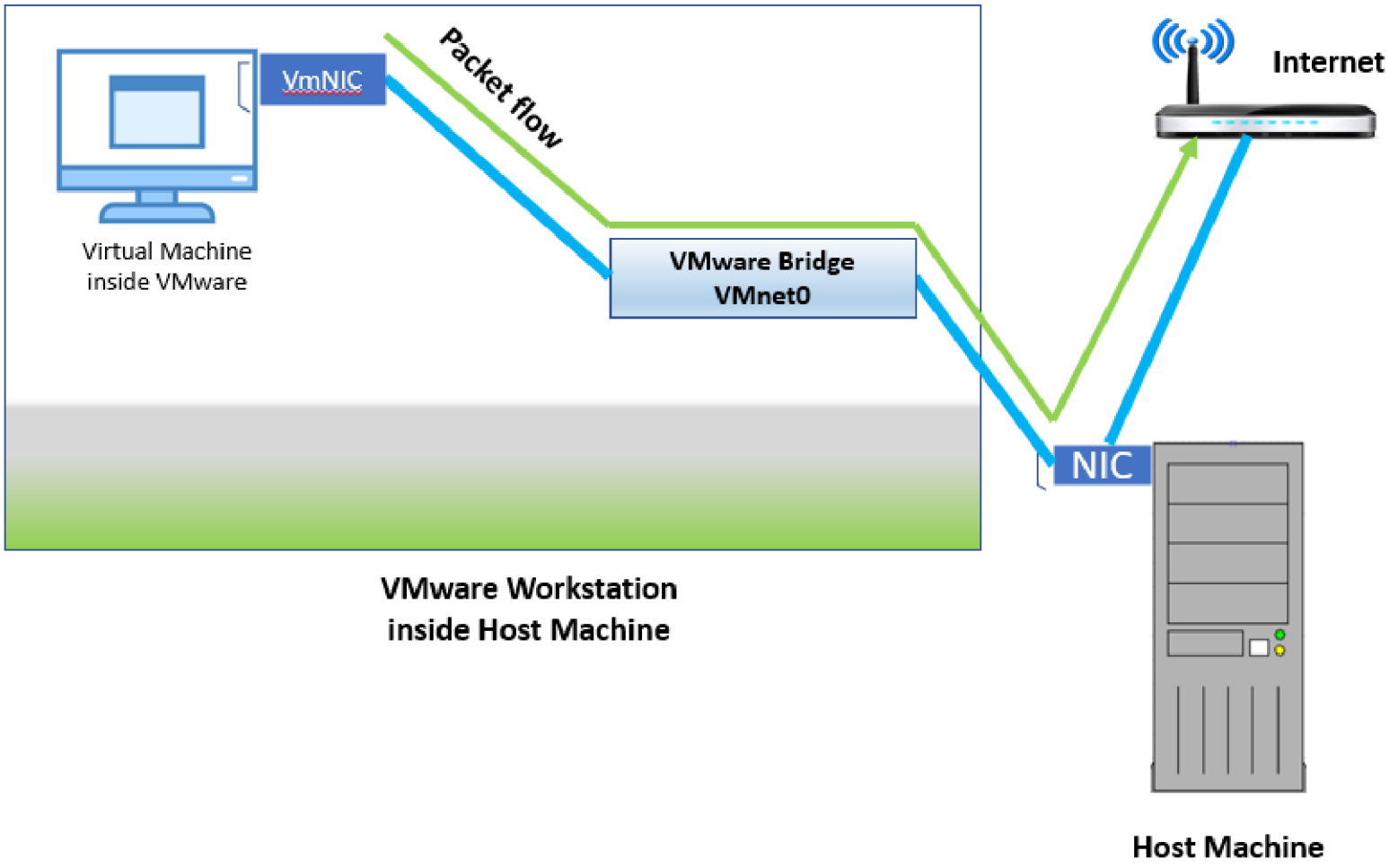
- **Two ways to connect VM to the Internet using VMware:**
  - Bridged network adapter (BNA).
  - Network Address Translation (NAT).

Connecting Malware to the Internet

- BNA allows VM to connect to the same LAN interface as the physical machine.

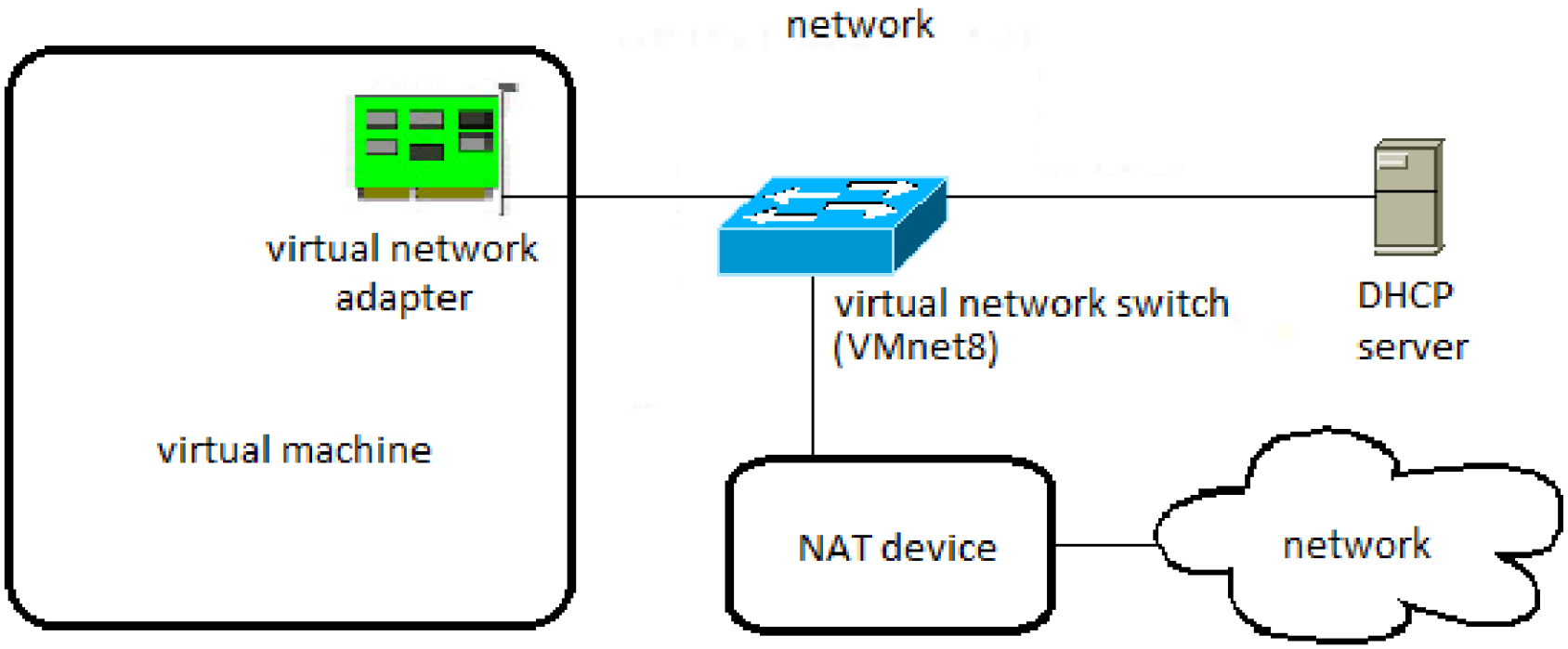
- NAT mode lets VMs see each other and the Internet but puts a virtual router between the VM and the LAN.

Connecting Malware to the Internet



Vmware bridged networking

Connecting Malware to the Internet



Vmware NAT networking

Connecting Malware to the Internet:

MORE ABOUT NAT MODE

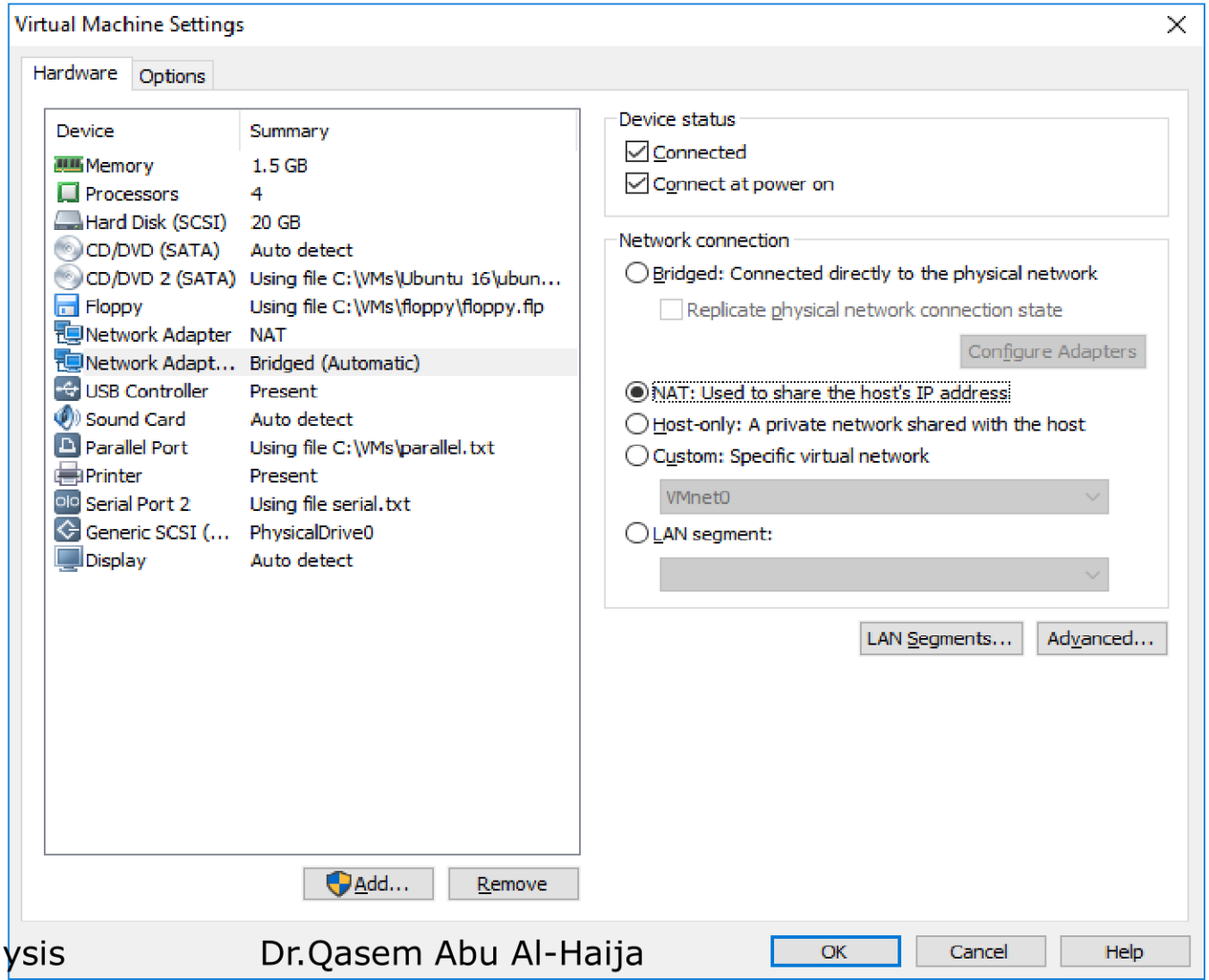
- NAT mode shares the host's IP connection to the Internet.
  - The host acts like a router and translates all requests from the VM so that they come from the host's IP address.
  - Useful mode for networks that do not allow connecting of VM adapter to the same network.

- Example: A host is using a wireless adapter
  - NAT allows VM to connect even: If the network is protected by WPA or WEP or If only certain adapters are allowed to connect,
  - Thus, NAT mode allows VM to connect through the host, avoiding the network's access control settings.

Connecting Malware to the Internet:

MORE ABOUT NAT MODE

We will use NAT mode for VM internet



Connecting and Disconnecting Peripheral Devices

- External devices such as CD-ROMs and USB storage drives.
  - Most devices can be connected to PM or VM, but not both.
  - VMware interface allows connecting/disconnecting them to VM.

- Example: Connecting USB device while VM window is active.
  - VMware will connect it to VM and not PM (may be undesirable).
  - This can be modified by VMWare settings: VM=> Settings=> USB Controller=> uncheck “Automatically connect new USB devices”.

Taking Snapshots

- VM snapshots allow you to save a computer's current state and return to that point later, like a Windows restore point.

- After you've installed your OS and malware analysis tools and you have configured the network, take a snapshot.
  - Use that snapshot as your base, clean-slate snapshot.
  - Next, run your malware, complete your analysis,
  - Then save your data and revert to the base snapshot,
  - You can do it all over again.

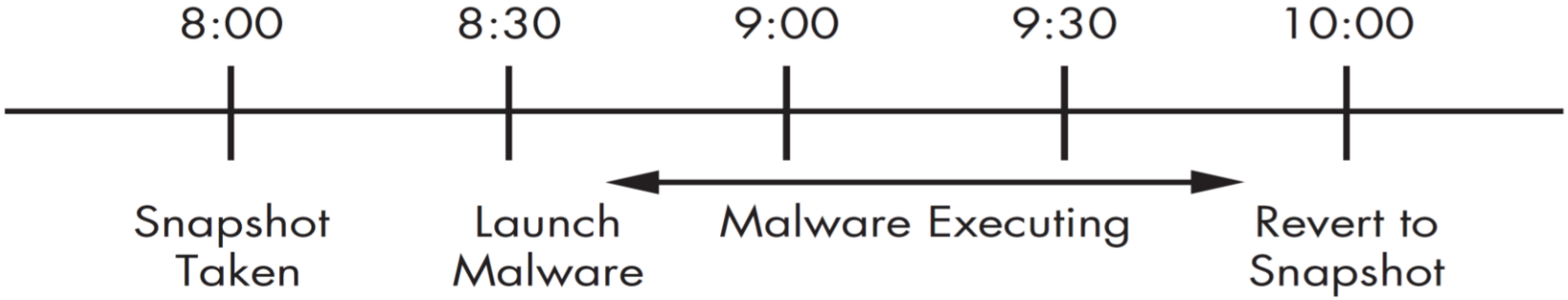


Figure 2-5: Snapshot timeline

Transferring Files from a VM

- One drawback of using snapshots:
  - Files on the VM are lost when you revert to an earlier snapshot.
- Solution: Transfer the required files to the host OS
  - Using VMware's drag-and-drop feature, or
  - Using VMware's shared folders accessible by host and guest OS.

Risks of Using VMware for Malware Analysis

- Malware may detect that it is in a VM and run differently
- VMware has bugs: malware may crash or exploit it
- Malware may spread or affect the host – don't use a sensitive host machine
- All the textbook samples are harmless

Summarized Steps Running and analyzing malware using VMware

1. Start with a clean snapshot with no malware running on it.
2. Transfer the malware to the virtual machine (VM).
3. Conduct your analysis on the virtual machine.
4. Take your notes, screenshots, and data from the VM and transfer them to the physical machine.
5. Revert the virtual machine to the clean snapshot.

LAB:

Preparing Your Virtual Environment

Downloading VMWare Player 16 for Windows

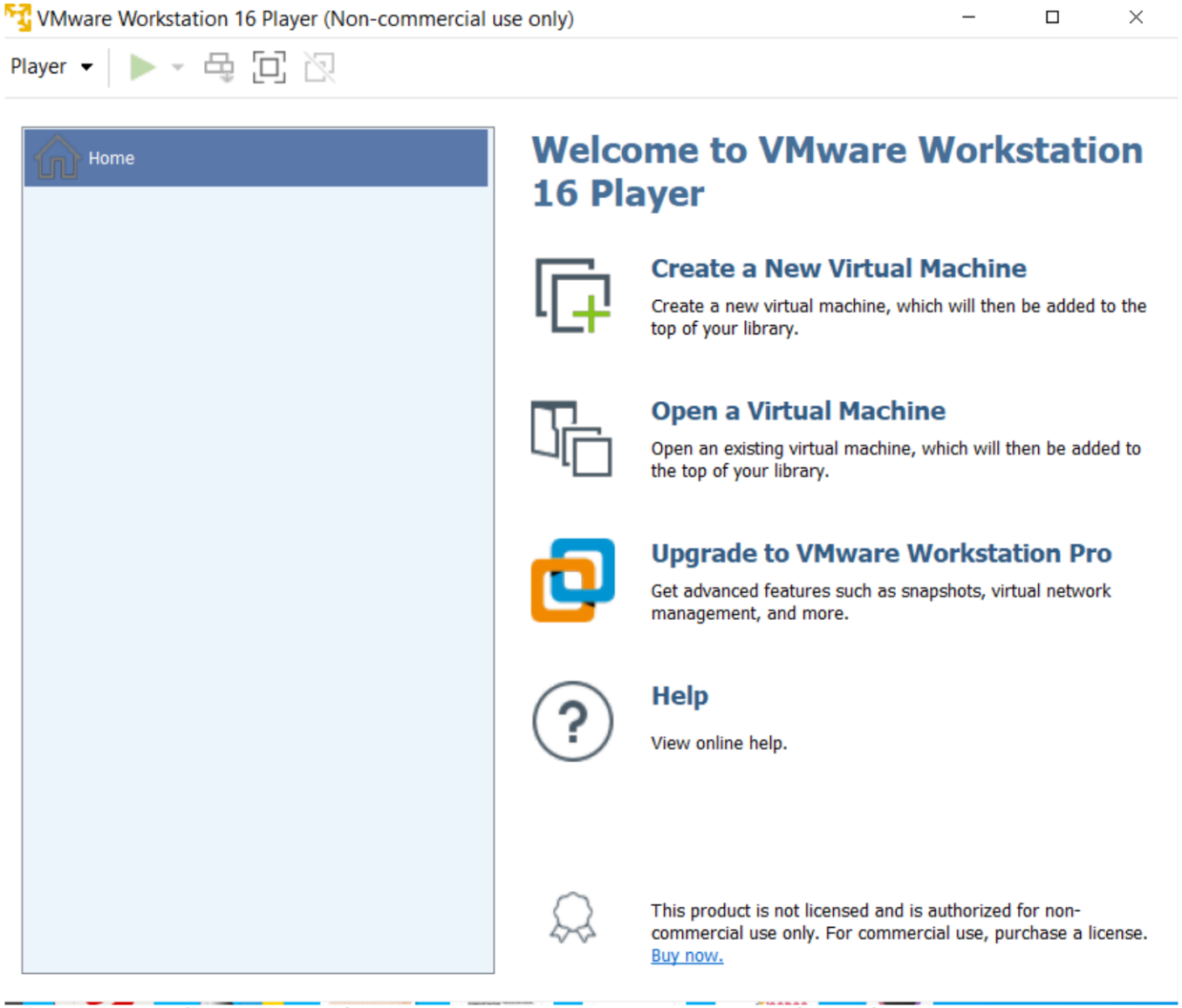
https://vmware-player.en.uptodown.com/windows

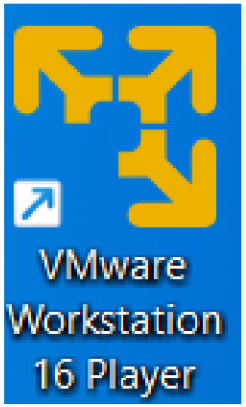
Try Workstation 16.0 Player for Windows

DOWNLOAD NOW >

VMware-player-full
-16.2.4-20089737

Installing VMWare Player 16 On Windows

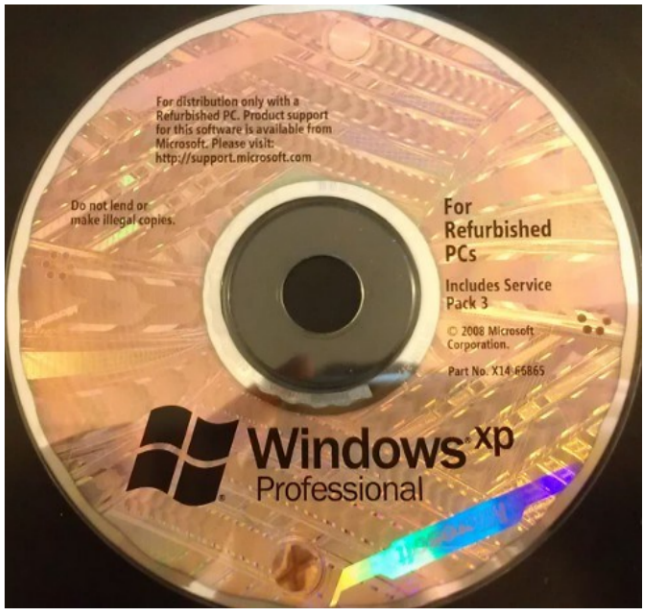


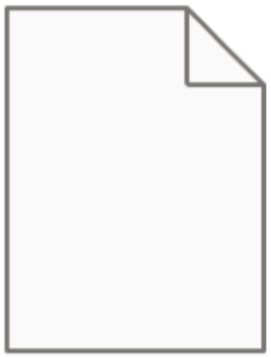


Downloading Windows XP

You need to Download Windows XP .ISO file and License

https://archive.org/details/WinXPProSP3x86



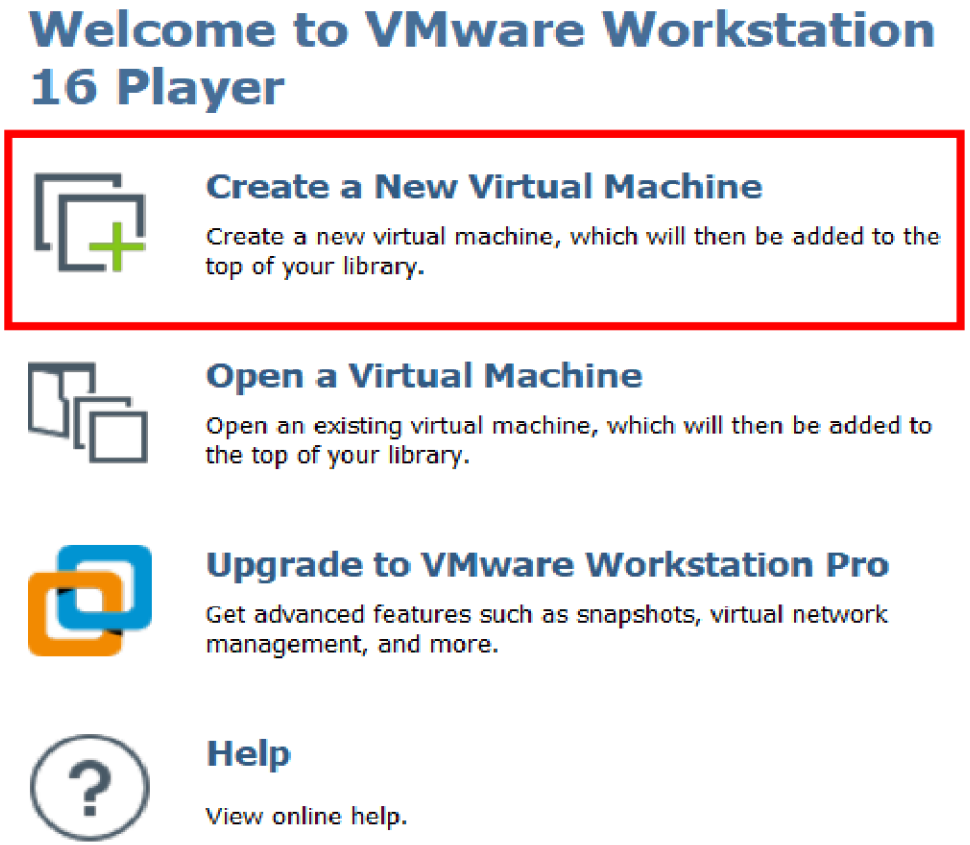


en_windows_xp_professional_with_service_pack_3_x86_cd_vl_x14-73974.iso

Serial: MRX3F-47B9T-2487J-KWKMF-RPWBY

Installing Windows XP Pro on VMWare

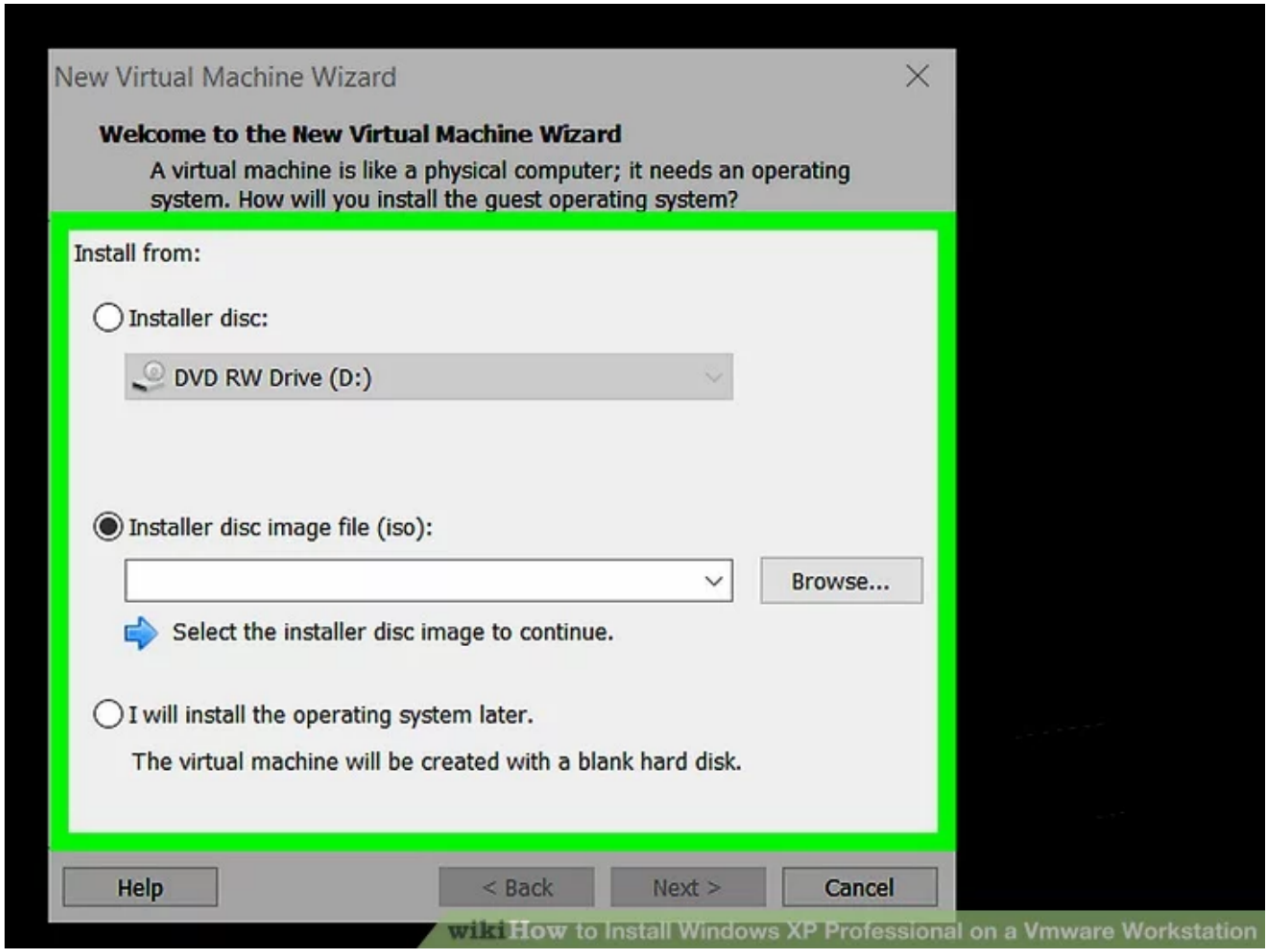
Open VMware, left click on Add New Virtual Machine to bring up the new virtual machine wizard to start the process.



Installing Windows XP Pro on VMWare

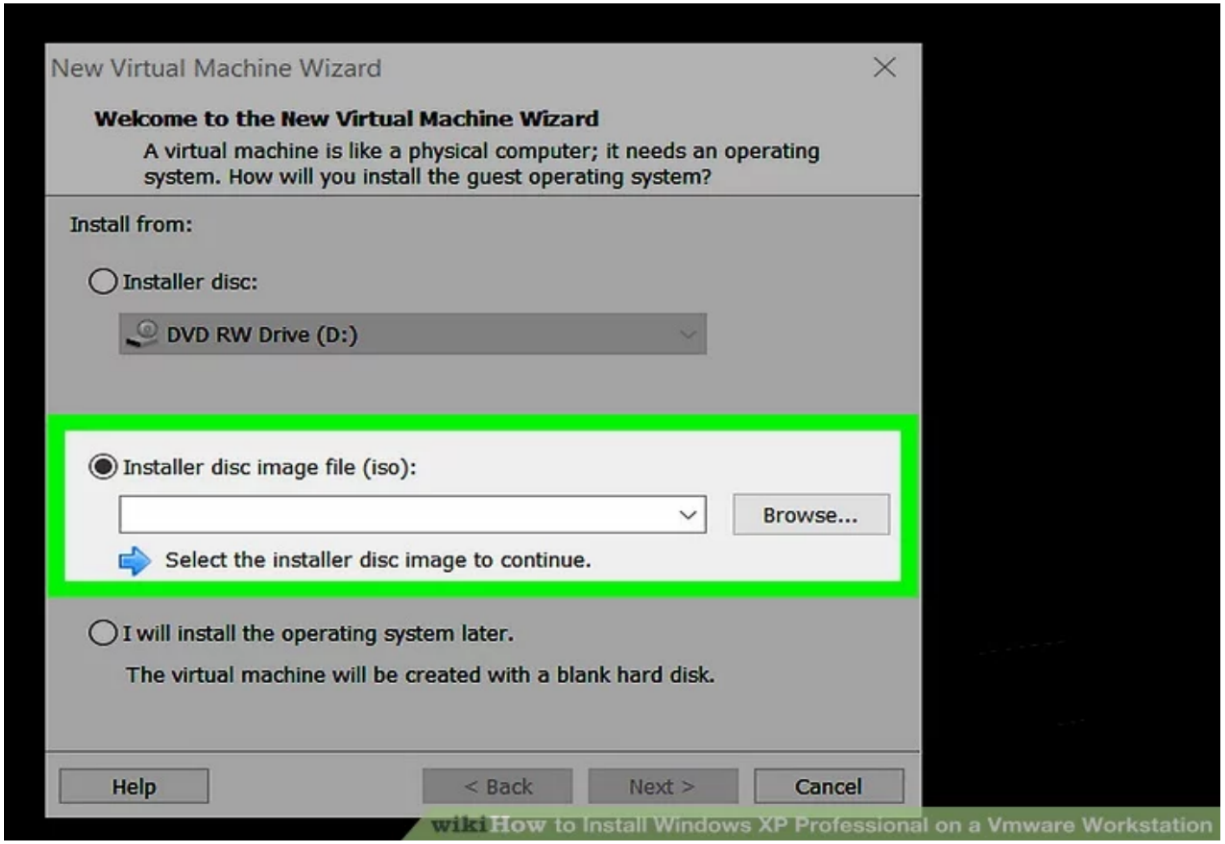
Left click on the typical (recommended) install option's radio button.

Left click on the next button.



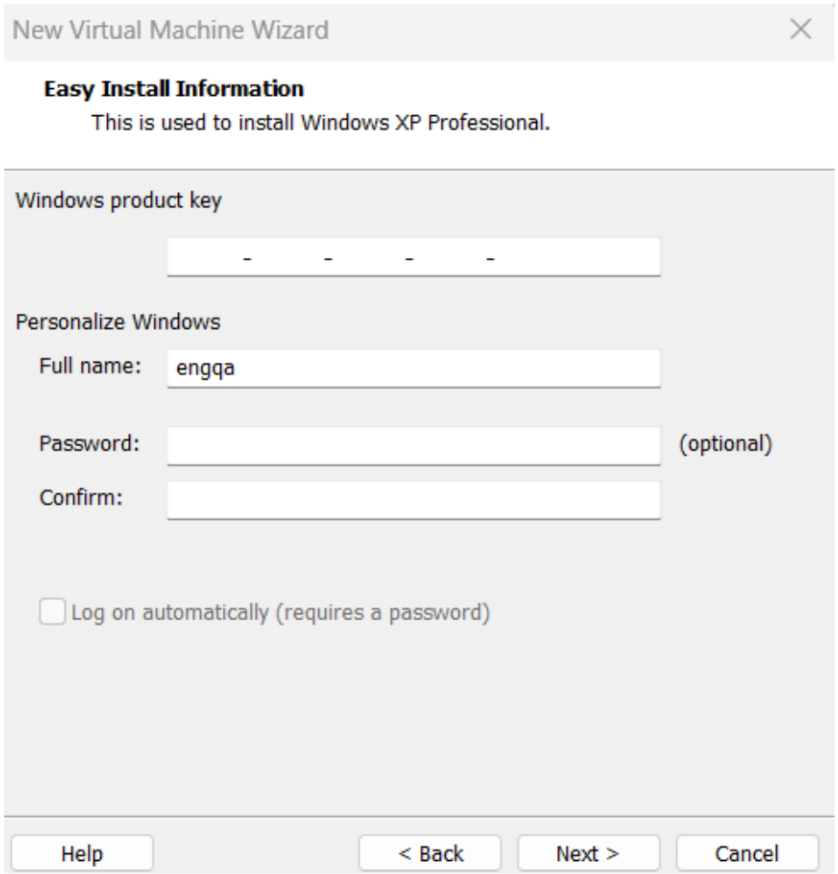
Installing Windows XP Pro on VMWare

Left-click on the Install Disc Image (ISO) radio button. Left-click on the browse button. Locate your Windows XP Professional ISO file and insert it in the option field. Left click the next button.



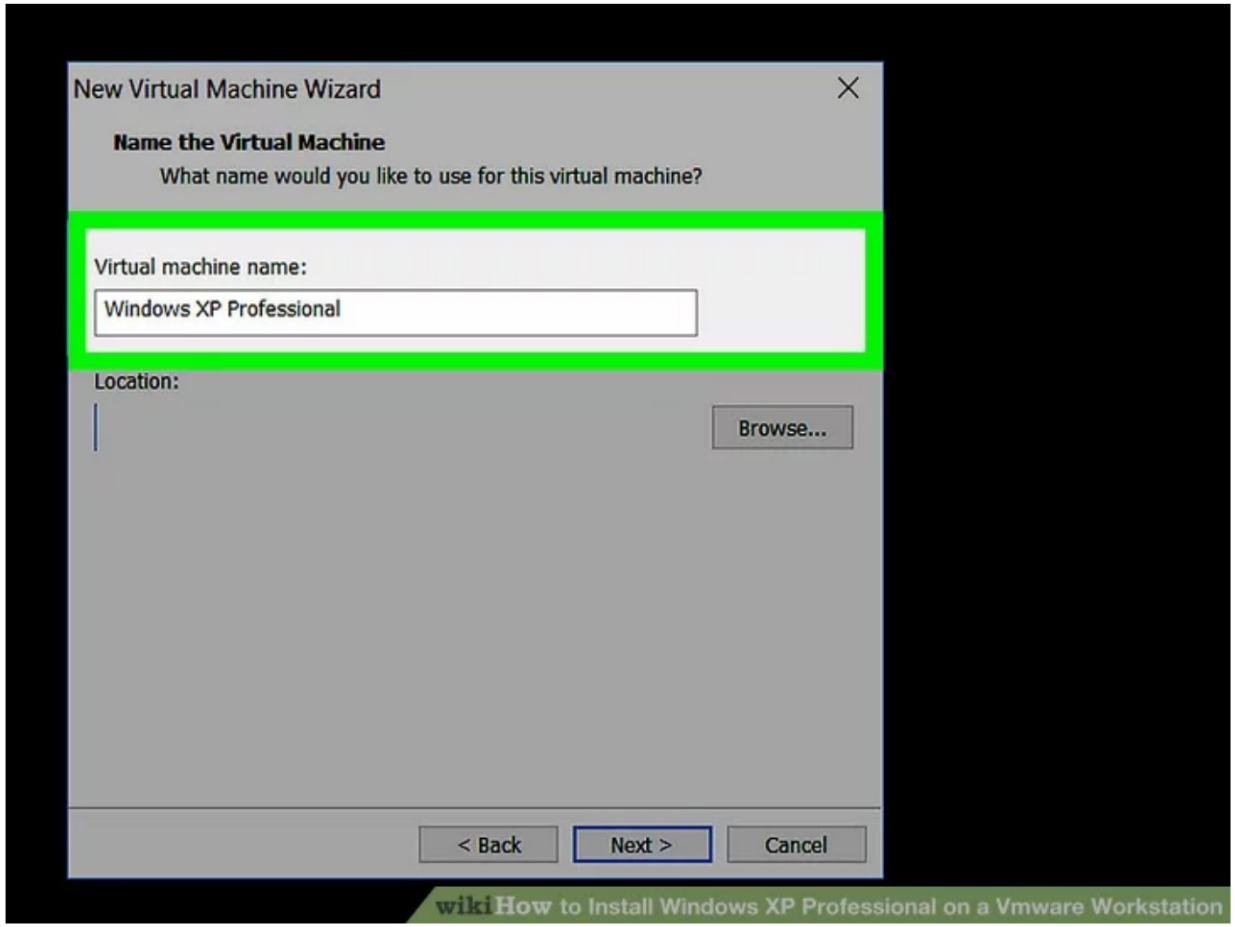
Installing Windows XP Pro on VMWare

Enter your Windows XP Product key. Enter a password if you would like, though it is optional. Left click on the next button.



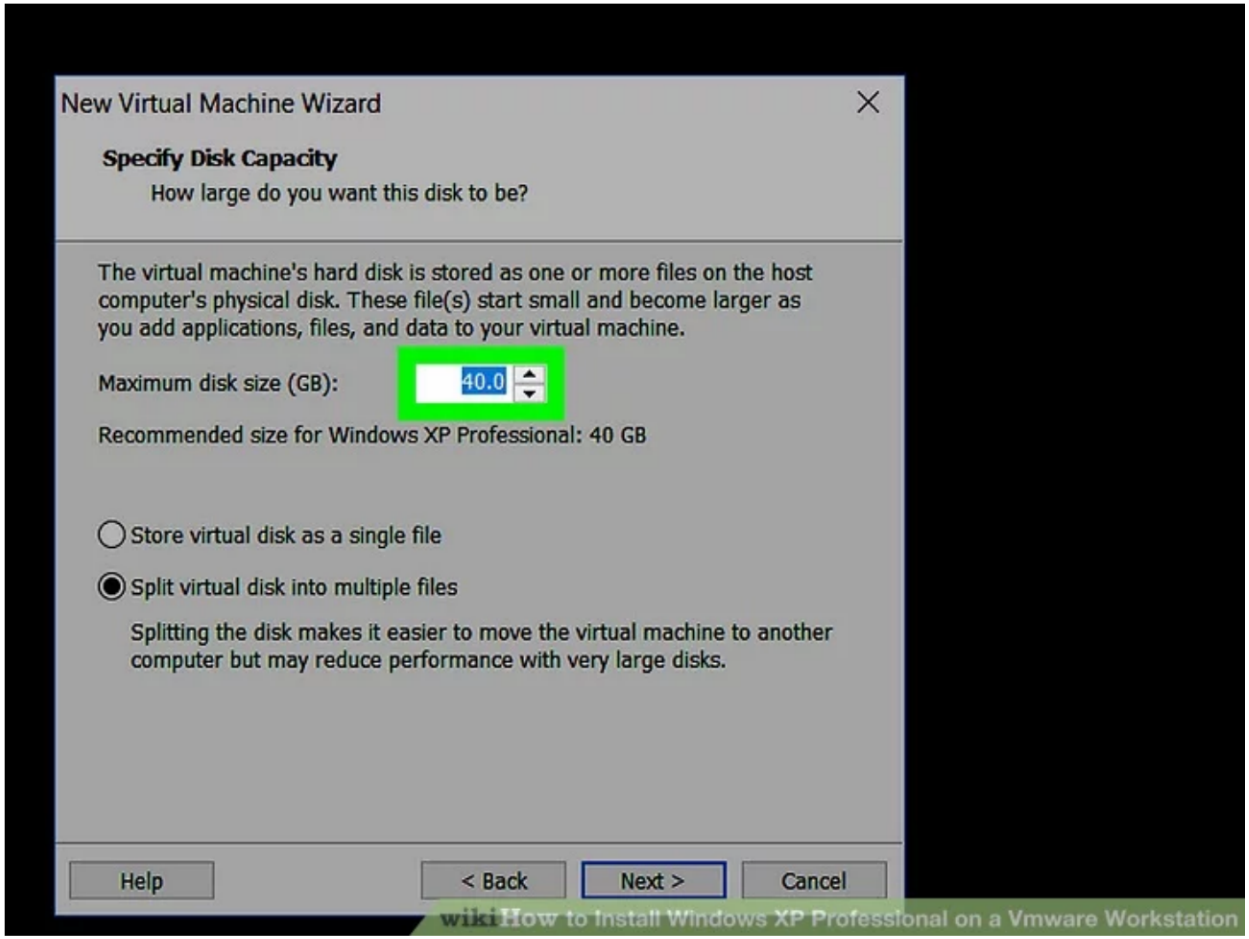
Installing Windows XP Pro on VMWare

Name your virtual machine whatever you would like in the Virtual Machine Name Field. Left click the next button.



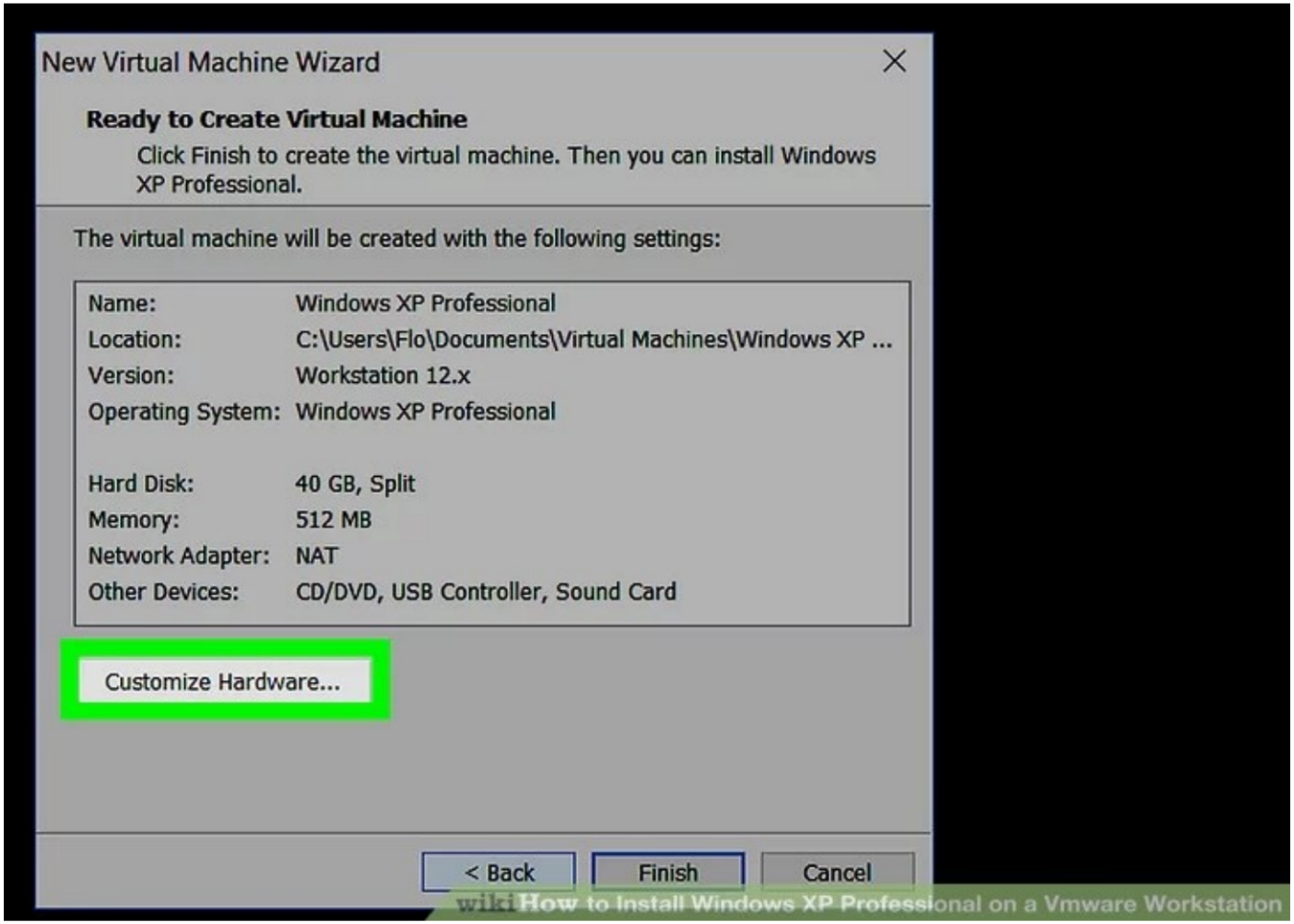
Installing Windows XP Pro on VMWare

Specify the amount of hard drive space you want to give to the Virtual Machine. *40 gigabytes is the recommended size* Left-click the next button.



Installing Windows XP Pro on VMWare

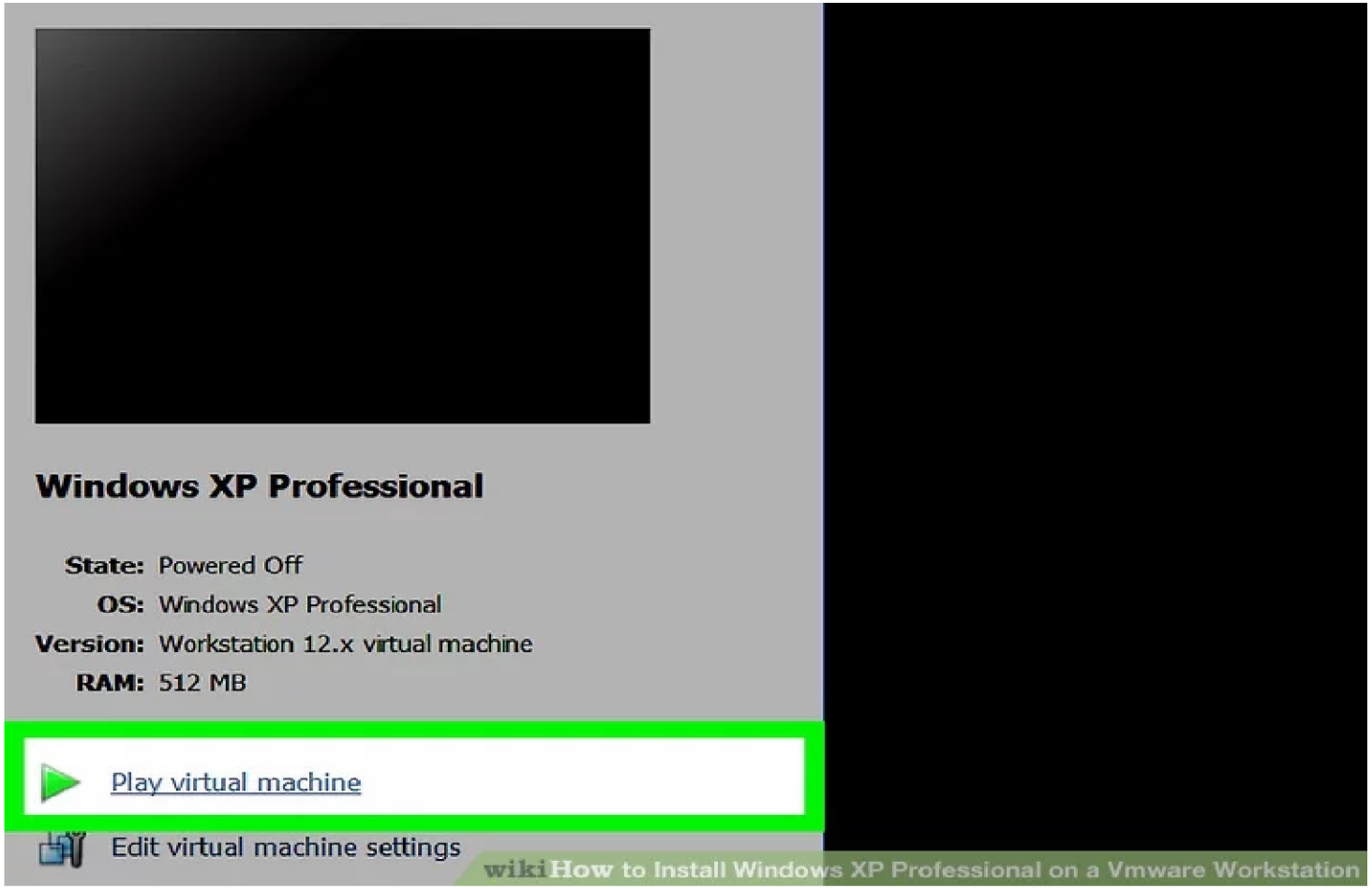
Review the list of specifications for your virtual machine. Left click on the finish button. The machine will start the install.



Installing Windows XP Pro on VMWare

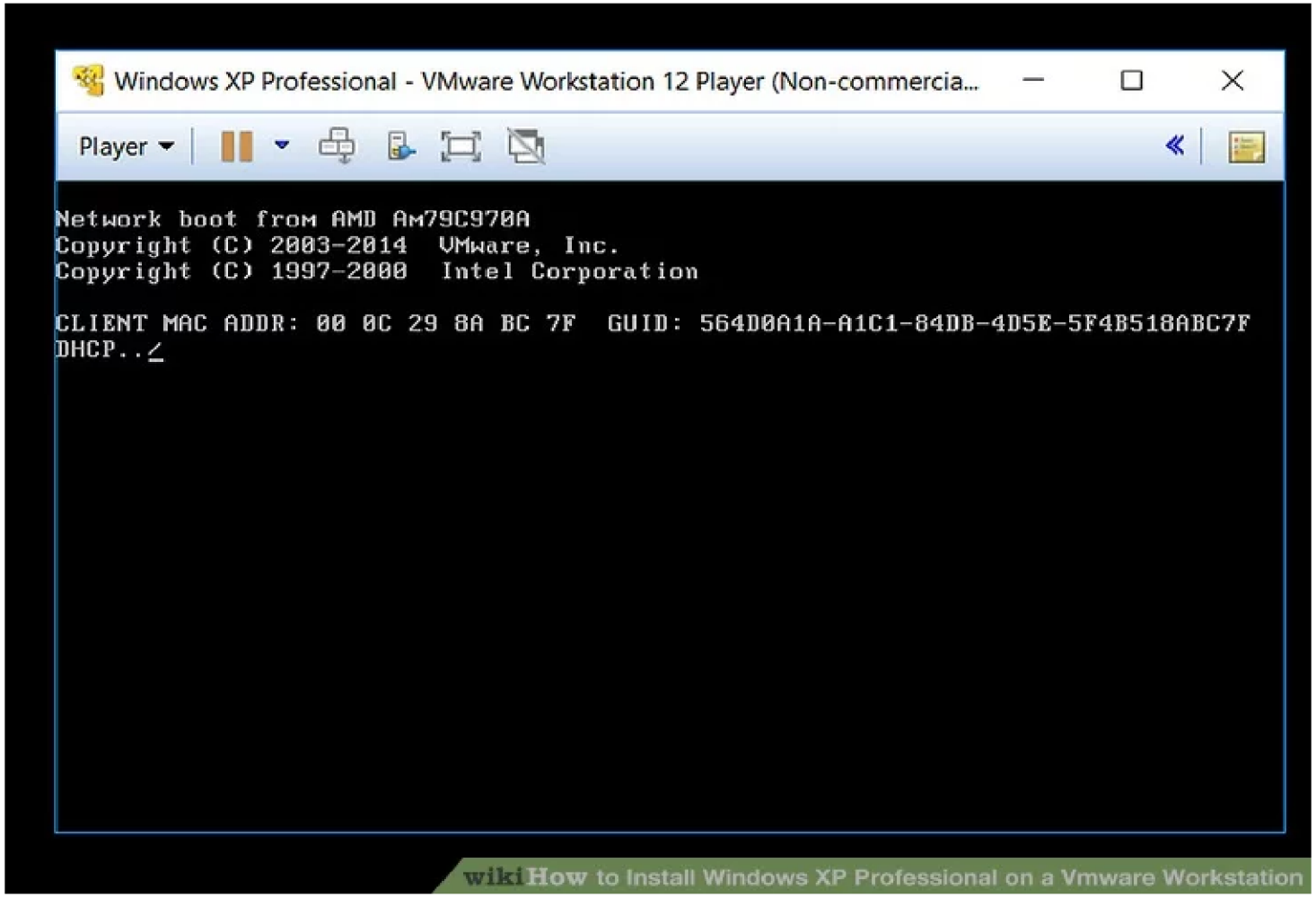
Let the installation run and the installation will boot up to the windows desktop.

Windows will prompt you to activate windows. Left click the "no" radio button.



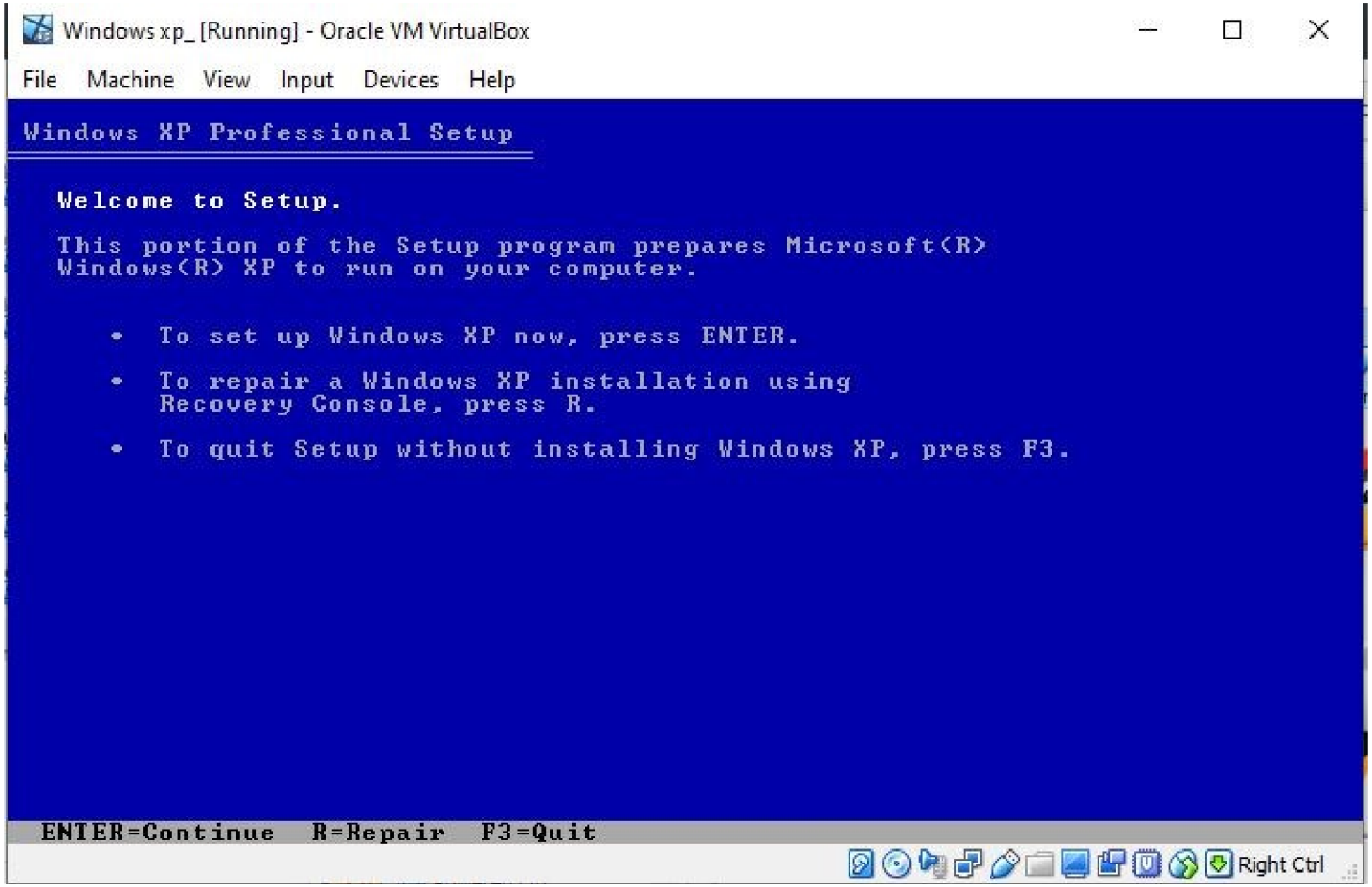
Installing Windows XP Pro on VMWare

Your Windows XP machine will restart to complete the installation.



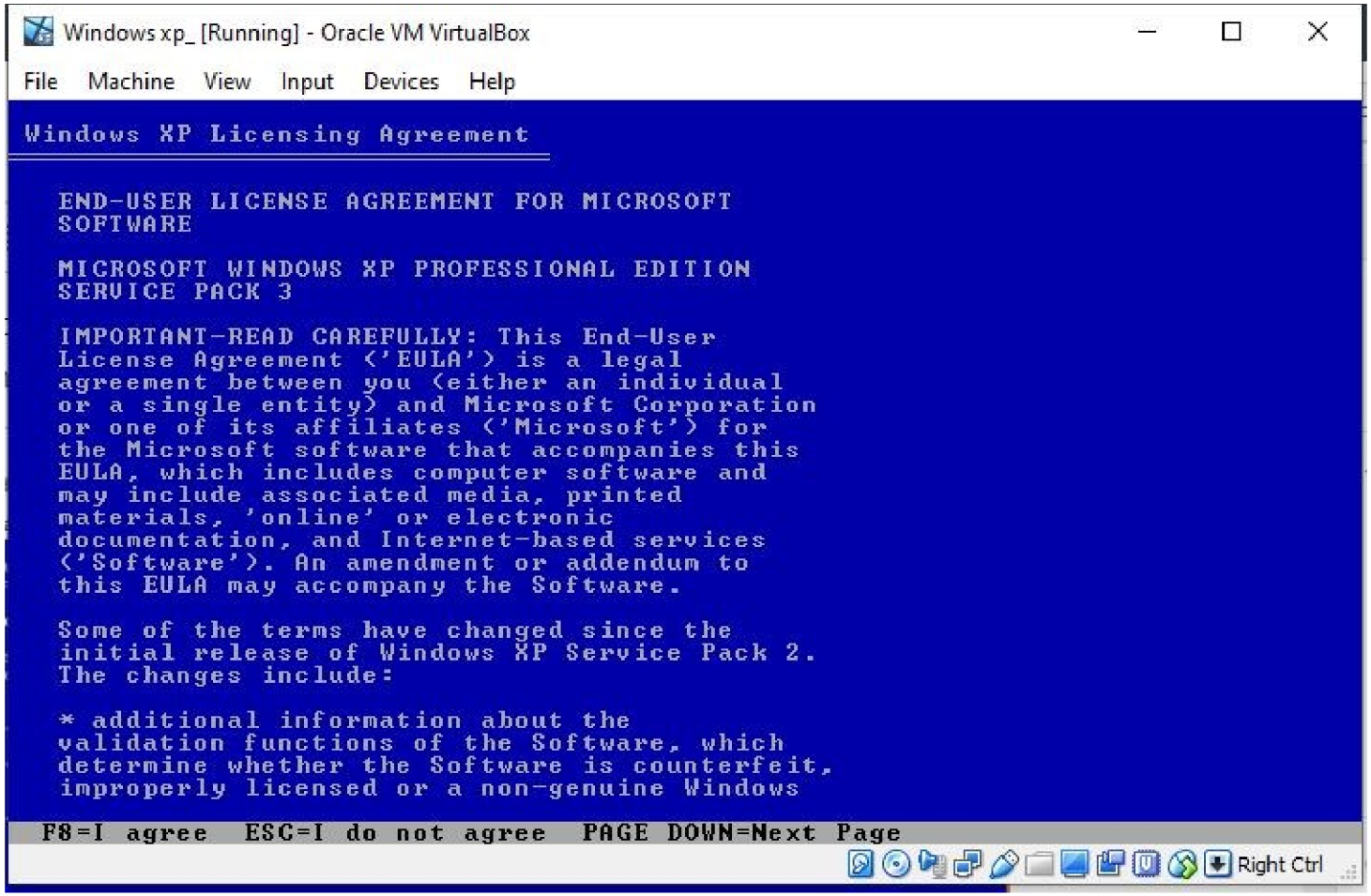
Installing Windows XP Pro on VMWare

Windows XP Professional Setup will open, press the Enter button to continue.



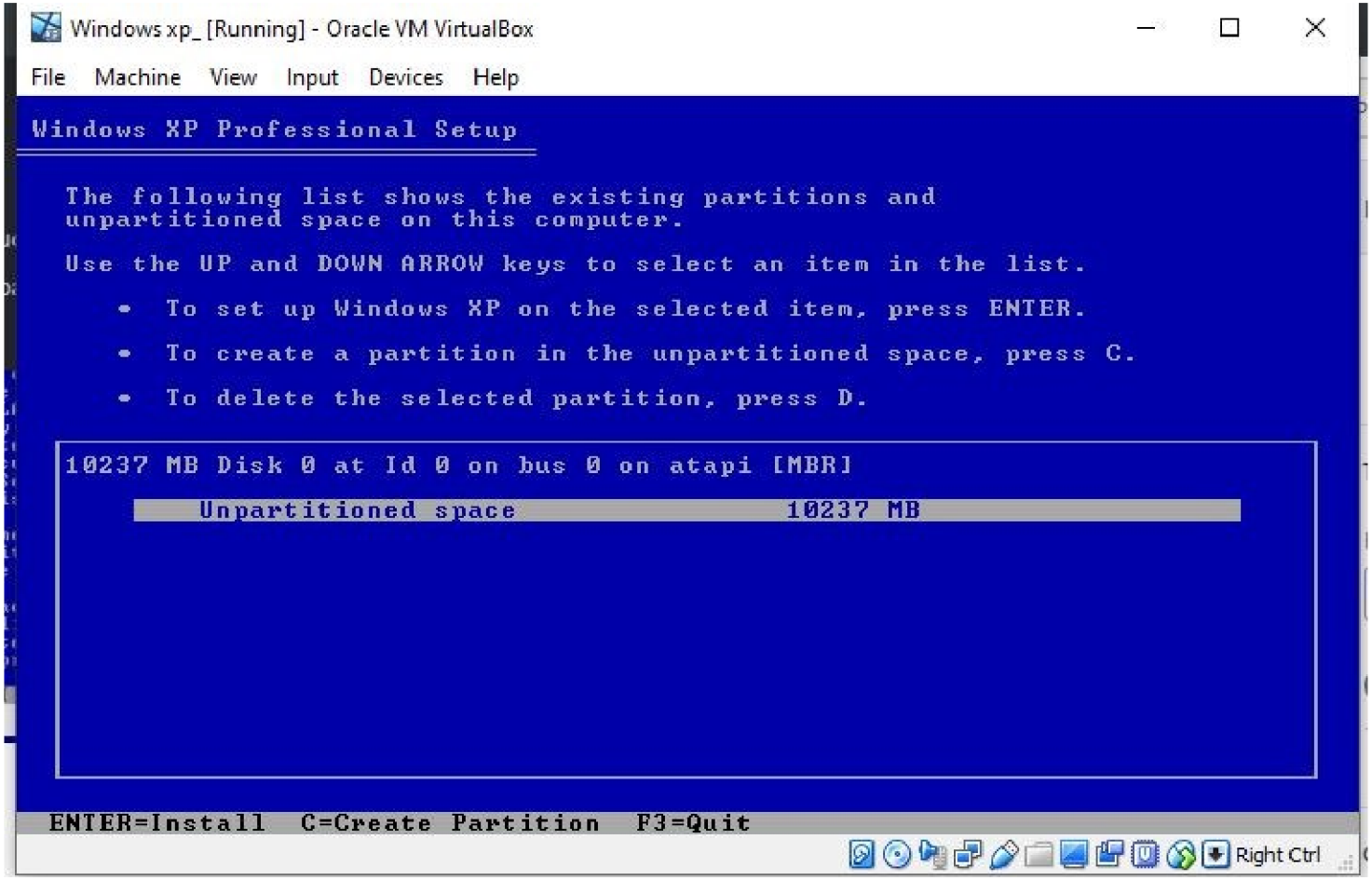
Installing Windows XP Pro on VMWare

Press F8 to accept the Windows XP Licensing Agreement.



Installing Windows XP Pro on VMWare

As we are installing Windows XP on VirtualBox, thus, a single partition will appear, simply press the enter button to format the whole partition.



Installing Windows XP Pro on VMWare

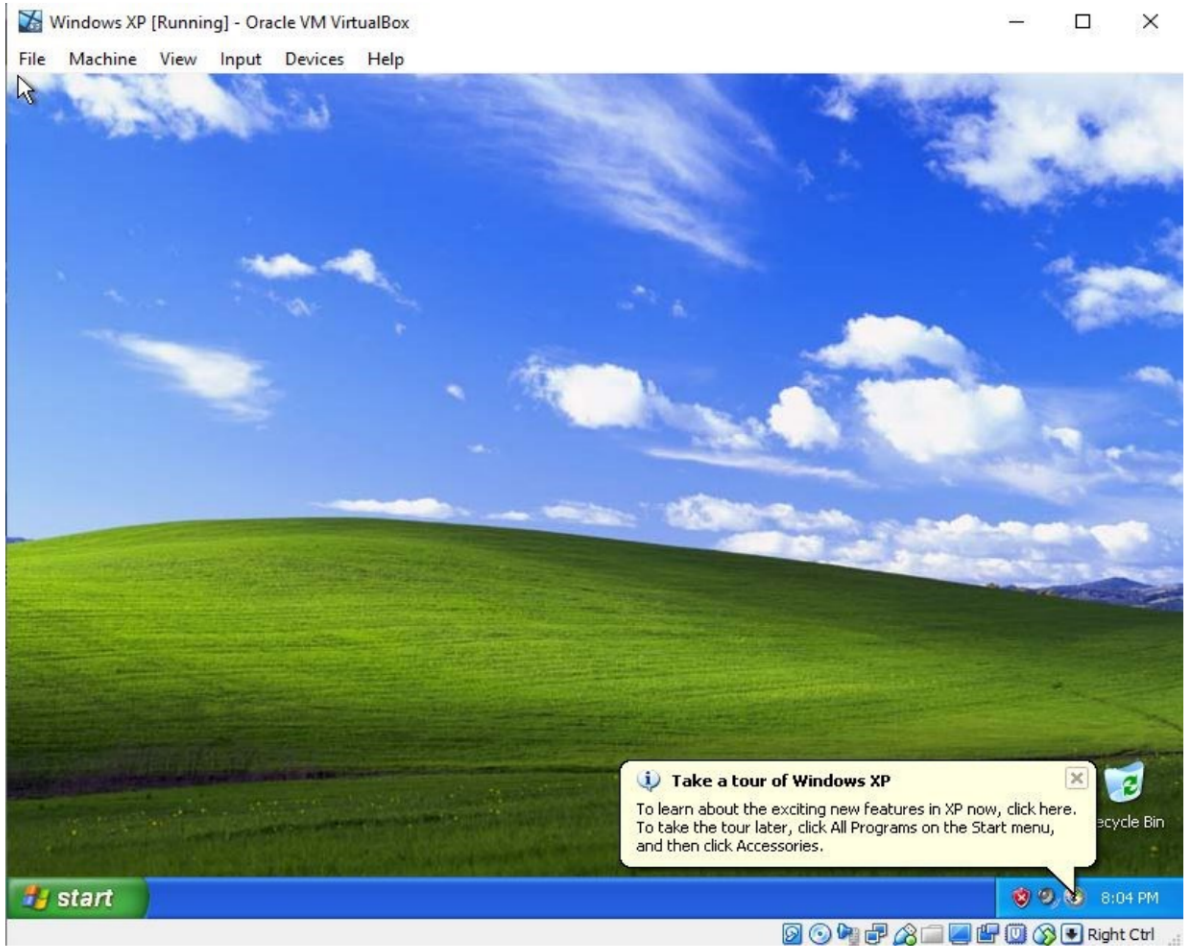
By default, slow formatting option will be selected, use the arrow key of the keyboard and select " Format the partition using the NTFS file system (Quick)".

Installing Windows XP Pro on VMWare

After some time, it will ask you to enter the license key for Windows XP. Type the official serial key: MRX3F-47B9T-2487J-KWKMF-RPWBY and click on the NEXT button to complete the installation.

Installing Windows XP Pro on VMWare

Once it will be done, you will get the old but very familiar interface of Windows XP with familiar startup sound.



Installing Windows XP Pro on VMWare

Once it will be done, you will get the old but very familiar interface of Windows XP with familiar startup sound.

Disabling Windows Security and Update Settings

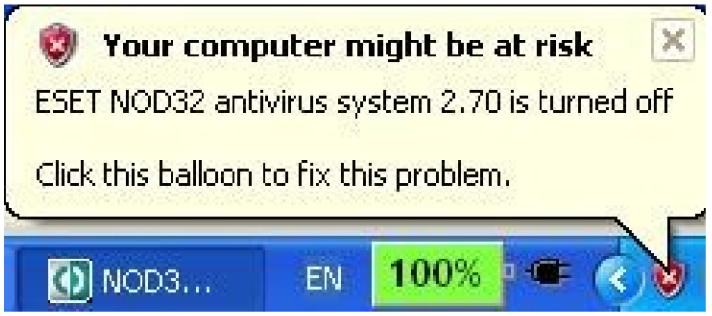
Go to control panel first then select Security Center

Disabling Windows Security and Update Settings

Windows XP has a built-in security center that monitors the activities or existence of Automatic Updates, Windows firewalls, and virus protection provided by third-party anti-virus software.

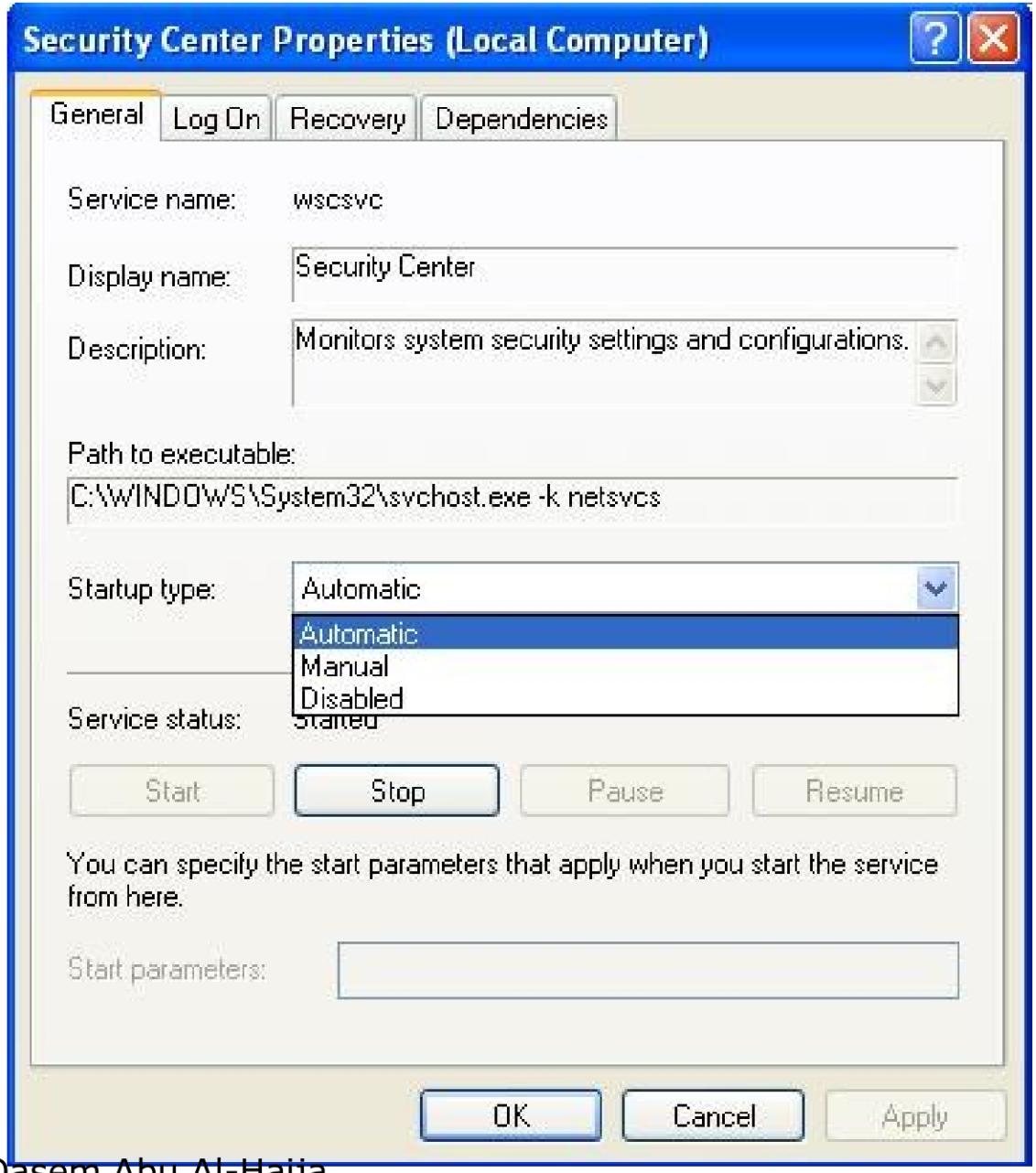
Disabling Windows Security and Update Settings

Security Center in Windows XP can be disabled or turned off so that the system will not monitor or check whether the antivirus software existed, is properly installed and running, or whether the firewall and Automatic Updates have been disabled or bypassed.



1. Click on **Start** button, then select **Control Panel**.
2. Select **Administrator Tools** (if you don't see it, double click on **Performance and Maintenance** first).
3. Double click **Services**.
4. Find and double-click on the service named **Security Center**. Alternatively right, click on **Security Center** and select **Properties** on right-click menu.
5. In the **General** tab, beside the **Startup type:** change the setting from Automatic to **Disabled**. This will permanently disable Security Center, even after you reboot and restart the computer system
6. Click on the Stop button at the bottom of the dialog window to stop Security Center immediately during the current log-on session.

Disabling Windows Security and Update Settings



Now, your VM is ready for Malware Analysis.

You can start installing and practicing the different Malware analysis tools

Main Sources for these slides

- *Michael Sikorski and Andrew Honig, "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software"; ISBN-10: 1593272901.*
- *Xinwen Fu, "Introduction to Malware Analysis," University of Central Florida*
- *Sam Bowne, "Practical Malware Analysis," City College San Francisco*
- *Abhijit Mohanta and Anoop Saldanha, "Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware," ISBN: 1484261925.*

Thank you